TUGAS AKHIR – KS141501

PEMBUATAN STANDAR OPERATING PROCEDURE KEAMANAN ASET INFORMASI BERDASARKAN KENDALI AKSES DENGAN MENGGUNAKAN ISO/IEC:27002:2013 PADA STUDI KASUS STIE PERBANAS SURABAYA

Ardhana Yudi Saputra
5212100027

Dosen Pembimbing 1:
Dr. Apol Pribadi S., S.T, M.T
Dosem Pembimbing 2:
Anisah Herdiyanti, S.Kom, M.Sc., ITIL

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

Final Project - KS141501

DEVELOPING STANDARD OPERATING PROCEDURE FOR INFORMATION ASSET SECURITY BASED ON ACCESS CONTROL REFER TO ISO/IEC:27002:2013 FRAMEWORK IN CASE STUDY STIE PERBANAS SURABAYA

Ardhana Yudi Saputra
NRP 5212 100 027

Supervisor 1:
Dr. Apol Pribadi S., S.T, M.T
Supervisor 2:
Anisah Herdiyanti, S.Kom, M.Sc., ITIL

INFORMATION SYSTEM DEPARTMENT
Information Technology Faculty
Institute of Technology Sepuluh Nopember
Surabaya 2016

LEMBAR PENGESAHAN

PEMBUATAN STANDAR OPERATING PROCEDURE KEAMANAN ASET INFORMASI BERDASARKAN KENDALI AKSES DENGAN MENGGUNAKAN ISO/IEC:27002:2013 PADA STUDI KASUS STIE PERBANAS SURABAYA

TUGAS AKHIR
Disusun untuk memenuhi Salah Satu Syarat Memperoleh Gelar
Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

ARDHANA YUDI SAPUTRA
5212 100 027

Surabaya, 14 Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr.Ir.Aris Tjahyanto, M.Kom
NIP.19660310 199102 1 001

LEMBAR PERSETUJUAN

PEMBUATAN STANDAR OPERATING PROCEDURE KEAMANAN ASET INFORMASI BERDASARKAN KENDALI AKSES DENGAN MENGGUNAKAN ISO/IEC:27002:2013 PADA STUDI KASUS STIE PERBANAS SURABAYA

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:
ARDHANA YUDI SAPUTRA
5212 100 027

Disetujui Tim Penguji: Tanggal Ujian : 14 Juli 2016
Periode Wisuda: September 2016

Dr. Apol Pribadi S., S.T, M.T (Pembimbing 1)

Anisah Herdiyanti, S.Kom., M.Sc., ITIL (Pembimbing 2)

Feby Artwodini M., S.Kom., M.T (Penguji 1)

Eko Wahyu Tyas D., S.Kom, MBA (Penguji 2)

PEMBUATAN STANDAR OPERATING PROCEDURE KEAMANAN ASET INFORMASI BERDASARKAN KENDALI AKSES DENGAN MENGGUNAKAN ISO/IEC:27002:2013 PADA STUDI KASUS STIE PERBANAS SURABAYA

Nama Mahasiswa	**: Ardhana Yudi Saputra**
NRP	**: 5212 100 027**
Jurusan	**: Sistem Informasi FTIF-ITS**
Dosen Pembimbing 1	**: Dr. Apol Pribadi S., S.T, M.T**
Dosen Pembimbing 2	**: Anisah Herdiyanti, S.Kom, M.Sc., ITIL**

ABSTRAK

Semakin meningkatnya penggunaan teknologi informasi saat ini menuntut lembaga pendidikan untuk menjaga aset informasi yang dimilikinya karena aset informasi merupakan salah satu aset yang vital bagi lembaga pendidikan termasuk salah satunya adalah Perbanas. Perbanas sebagai salah satu sekolah tinggi memiliki beberapa aset informasi yang digunakan sebagai sebagai daya dukung tidak hanya untuk proses administrasi oleh para staff namun juga sebagai penunjang keberlangsungan proses belajar mengajar antara dosen dan mahasiswa. Namun salah satu masalah yang masih sering dihadapi oleh perbanas saat ini adalah keamanan akses aset informasi di bidang akademiknya. Tidak dapat dipungkiri bahwa lemahnya sistem keamanan akses aset informasi bisa menimbulkan ancaman bagi lembaga itu sendiri maupun orang-orang yang terlibat dalam sistem tersebut sehingga dapat mengganggu kegiatan yang menggunakan teknologi informasi. Maka dari itu diperlukan pengelolaan kendali akses aset informasi yang berbasis risiko yang dibentuk dalam sebuah

prosedur kendali akses aset informasi untuk mengelola kelemahan maupun ancaman yang muncul. Basis yang digunakan dalam membuat prosedur kendali akses aset informasi sebagai manajemen risiko adalah ISO/IEC:27002:2013. ISO/IEC:27002:2013 adalah framework sistem manajemen yang bisa dijadikan pedoman dalam mengelola keamanan aset informasi. Prosedur keamanan aset informasi yang dibuat ini dititikberatkan pada kendali akses yang merupakan salah satu kendali kemananan dari ISO/IEC:27002:2013. Dengan harapan setelah dibuat tata kelola keamanan aset informasi tersebut, maka dapat membantu dalam mengelola keamanan sistem informasi yang ada di Perbanas.

Kata Kunci : Standard Operating Procedure, Aset Informasi, , Kendali Akses, ISO/IEC:27002:2013.

DEVELOPING STNADARD OPERATING PROCEDURE FOR INFORMATION ASSET SECURITY BASED ON ACCESS CONTROL REFER TO ISO/IEC:27002:2013 FRAMEWORK IN CASE STUDY STIE PERBANAS SURABAYA

Name : Ardhana Yudi Saputra
NRP : 5212 100 027
Department : Information System FTIF-ITS
Supervisor 1 : Dr. Apol Pribadi S., S.T, M.T
Supervisor 2 : Anisah Herdiyanti, S.Kom, M.Sc., ITIL

ABSTRACT

The increasing use of information technology today requires educational institutions to safeguard its information assets for information assets is one of the assets that are vital to educational institutions, including one of which is the Banks Association. Banks Association as one of the high schools have some information assets that are used as a carrying capacity not only to the administrative process by the staff but also as supporting the continuity of the learning process between students and lecturers. But one of the problems that are often faced by Banks Association today is the access security of information assets in the academic field. It is inevitable that the weakness of the security system access information assets could pose a threat to the institution itself and the people involved in the system so that it can interfere with activities that use information technology. Thus it is necessary to manage the access control information assets based on risk, which is formed in an access control procedures for managing information assets weaknesses and emerging threats. The base used in making access control procedures as the risk management of information assets is an ISO / IEC: 27002: 2013. ISO / IEC: 27002: 2013 is a management system framework that can be used as guidance in managing the

security of information assets. Security procedures created information assets is focused on the access control is one security control of ISO / IEC: 27002: 2013. With the hope of once created governance of the security of information assets, it can be helpful in managing the security of information systems that exist in the Banks Association.

Keywords: Standard Operating Procedure, Information Asset, Access control, ISO/IEC:27002:2013

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini, teknologi informasi merupakan salah satu komponen yang sangat penting dalam menunjang keberlangsungan bisnis suatu orgnaisasi maupun perusahaan dimana di dalam teknologi informasi tersebut juga terdapat aset informasi. Banyak perusahaan atau organisasi yang bergantung pada aset informasi yang dimilikinya. Semakin banyak pula organisasi yang menyadari bahwa informasi memiliki potensi untuk memberikan keunggulan kompetitif serta menjadi pendukung kesuksesan organisasi tersebut. Pentingnya nilai sebuah informasi membuatnya hanya dapat diakses oleh orang-orang tertentu saja, karena apabila jatuh ke tangan yang salah maka dapat menimbulkan kerugian bagi organisasi pemilik informasi tersebut (Sarno & Iffano, 2009). Informasi tersebut bisa berupa data karyawan, data pribadi organisasi, maupun data-data rahasia milik organisasi lainnya. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat juga menjadi sangat penting bagi organisasi. Karena itulah informasi saat ini telah menjadi bagian yang sangat penting dan tidak terpisahkan bagi kelangsungan sebuah organisasi.

Pentingnya akses informasi penting tersebut menyebabkan setiap perusahaan maupun organisasi wajib menjaga keamanan informasi yang dimilikinya Tidak terkecuali terhadap keamanan teknologi informasi yang dimiliki oleh lembaga-lembaga pendidikan salah satunya adalah STIE Perbanas. STIE Perbanas telah menggunakan teknologi informasi sebagai pendukung proses bisnis yang dijalankan, salah satu teknologi informasinya adalah sistem akademik.

Salah satu wakil rektor bagian akademik yang ada di perbanas bernama Didik pun menuturkan jika sistem keamanan yang ada di perbanas ini pun masih lemah, salah satu contohnya adalah pernah terjadi pembajakan terhadap sistem informasi akademik yang ada di perbanas dan juga penembusan jaringan wifi milik jajaran manajemen yang dilakukan oleh mahasiswa sehingga menimbulkan kerugian bagi salah satu pihak, maka dari itu dibutuhkan dukungan terhadap keamanan aset informasi yang tujuannya adalah agar informasi yang dimiliki terjamin kerahasiaannya (confidentiality), keutuhannya (integrity), dan ketersediannya (availability).

Untuk mencegah pencurian data yang dapat mengakibatkan bocornya informasi penting, organisasi perlu memiliki sebuah kontrol untuk membatasi informasi apa saja yang dapat dilihat dan diakses. Pada tahun 2011, DataLossDB mencatat ada 88 insiden terkait dengan aksesbilitas web yang terjadi pada organisasi swasta maupun pemerintah, dengan presentase 8% dari keseluruhan 1041 insiden yang mengakibatkan hilangnya data di sebuah organisasi (DataLossDB, 2011). Dengan memiliki kontrol terhadap akses aset informasi, organisasi dapat meminimalkan kerugian yang diakibatkan oleh hilangnya data yang disebabkan oleh penyalahgunaan akses.

Dalam melakukan akses terhadap informasi yang penting yang ada di STIE Perbanas Surabaya, dibutuhkan suatu izin pemberian hak akses terhadap informasi tersebut. Sehingga dalam menginisiasi sebuah keamanan informasi, perlu bagi organisasi ini untuk memastikan keamanan akses dan juga penggunaan dari hak akses oleh masing-masing orang yang berhak terhadap akses yang dimilikinya. Karena

pada kenyataannya masih ada penyelewengan terhadap penggunaan hak akses yang bisa menyebabkan kerugian bagi STIE Perbanas maupun masing-masing elemen dalam STIE Perbanas. Penyelewengan ini bukan hanya dikarenakan oleh pencurian hak akses yang dilakukan oleh suatu pihak dengan tujuan mendapatkan informasi maupun data yang dicari, namun juga masih kurangnya kesadaran masing-masing pemilik hak akses terhadap pentingnya izin akses tersebut. Salah satu contoh penyelewengan hak akses ini adalah masih adanya pertukaran password antar mahasiswa agar bisa mengakses informasi yang sebenarnya bukan kewenangan dari mahasiswa tersebut, hal ini bisa terjadi karena alasan kepercayaan pertemanan sehingga mahasiswa merasa tidak ada masalah terhadap pemeberian kewenangan hak akses miliknya tersebut padahal faktanya banyak risiko yang bisa terjadi yang bisa merugikan salah satu pihak maupun keduanya karena penggunaan hak akses yang bukan wewenangnya tersebut. Hal mengenai hal akses ini perlu diberi perhatian khusus karena hak akses itulah yang merupakan kunci dari seseorang untuk bisa mengakses data dan informasi yang ada di dalamnya sehingga diperlukan kendali terhadap akses tersebut agar penggunaannya bisa digunakan sesuai dengan hak akses masing-masing. Permasalahan mengenai kendali akses ini bisa diselesaikan dengan membuat sebuah prosedur yang baik untuk memastikan tidak adanya risiko yang berulang kembali yang bisa menyebabkan terganggunya proses bisnis yang berjalan dan kerugian oleh pihak-pihak tertentu.

Mengingat permasalahan yang dimiliki oleh STIE Perbanas adalah mengenai keamanan informasi yang berkaitan dengan kendali akses dan juga untuk menjaga keamanan informasi yang dimiliki oleh STIE Perbanas, maka diperlukan dukungan untuk menjaga

keamanan data dan informasi yang ada di STIE Perbanas yang berdasarkan pada penelitian sebelumnya dengan cara merancang dokumen SOP *(Standard Operating Procedure)* keamanan aset informasi mengenai kendali akses agar risiko yang mungkin bisa menimpa setiap aset keamanan informasi bisa diminimalisir maupun dihindari, sehingga tidak mengganggu keberlangsungan proses bisnis yang dijalankan oleh STIE Perbanas dan seluruh data yang dimiliki menjadi aman. SOP ini berguna dalam mendefinisikan seluruh konsep, teknik, dan persyaratan dalam melakukan suatu proses yang dituliskan ke dalam suatu bentuk yang langsung dapat digunakan oleh pegawai yang bersangkutan dalam melaksanakan tugas proses bisnisnya (R Stup, 2002). Disamping itu dengan adanya kebijakan keamanan informasi, maka organisasi dapat menetapkan dan memberikan perlindungan keamananan yang tepat dan efektif. Informasi yang memiliki tingkat keamanan paling tinggi akan memerlukan kontrol dan perlindungan yang paling ketat, sementara yang berklasifikasi biasa juga akan diberikan perlindungan yang sesuai. Kebijakan maupun prosedur pengamanan keamanan informasi khususnya dalam hal kendali akses ini akan ditetapkan dengan mempertimbangkan klasifikasi analisa risiko yang akan dilakukan nantinya.

Pada proses pembuatan sebuah dokumen SOP ini dibutuhkan adanya standard yang akan menjadi sebuah acuan. Pada penelitian yang dilakukan kali ini, kerangka kerja yang akan digunakan adalah standard ISO/IEC 27002:2013 yang mana ISO/IEC 27002:2013 akan digunakan sebegai penentuan kontrol yang harus ada dalam penyusunan dokumen SOP terutama kontrol yang berkaitan dengan kendali akses pada hasil risiko yang memiliki tingkat kerentanan *very high* dan juga *high.*

1.2 Perumusan Masalah

Permasalahan yang akan diselesaikan dalam tugas akhir ini adalah sebagai berikut:

1. Apakah hasil analisis risiko keamanan aset informasi yang berhubungan dengan kendali akses yang ada di STIE Perbanas Surabaya?
2. Bagaimana hasil pembuatan dokumen SOP *(Standard Operating Procedure)* untuk kendali akses yang mengacu pada kontrol kerangka kerja ISO/IEC 27002:2013?
3. Bagaimana hasil verifikasi dan validasi terhadap dokumen SOP kendali akses dengan kebutuhan keamanan yang diperlukan di STIE Perbanas?

1.3 Batasan Masalah

Batasan masalah pada Tugas Akhir ini adalah :

1. Penelitian ini berfokus pada kontrol kerangka kerja ISO/IEC 27002:2013 yaitu pada *A.9 Access Control* dan subnya yang sesuai dengan hasil analisa risiko yang sudah dilakukan
2. Justifikasi dari analisis risiko dilakukan berdasarkan hasil wawancara dan interview langsung dengan Wakit Ketua 1 bidang Akademik dan Ketua Sie (Kasie) TIK STIE Perbanas.
3. Aset Informasi pada penelitian kali ini meliputi sumber daya manusia, data dan juga software.
4. Lingkup aset informasi yang berupa data pada penelitian ini adalah data demografi mahasiswa, data akademik dan data file server
5. Lingkup aset informasi yang berupa software pada penelitian ini adalah SIMAS, E-learning, dan perpustakaan.

1.4 Tujuan Tugas Akhir

Tujuan dari Tugas Akhir ini adalah sebagai berikut :

1. Mengetahui risiko-risiko apa saja yang dapat mengancam seluruh aset yang berkaitan dengan kendali akses dan mengetahui tindakan yang harus dilakukan untuk mengatasi risiko tersebut yang ada di STIE Perbanas Surabaya
2. Menghasilkan dokumen SOP *(Standard Operating Procedure)* kendali akses pada STIE Perbanas yang berdasarkan hasil analisis risiko dan sesuai dengan kerangka kerja ISO/IEC 27002:2013
3. Mengetahui hasil verifikasi dan validasi dari dokumen SOP sehingga dapat digunakan oleh STIE Perbanas untuk mendukung pengelolaan kendali akses.

1.5 Manfaat Kegiatan Tugas Akhir

Manfaat yang didapatkan dari penelitian adalah sebagai berikut:

1. STIE Perbanas mendapatkan hasil identifikasi aset-aset apa saja yang penting yang perlu dilindungi agar keamanan aset informasi tetap terjaga dengan aman.
2. STIE Perbanas mendapatkan hasil analisa risiko dan juga mitigasi mengenai tiap-tiap aset penting yang perlu mendapatkan perhatian khusus demi menjaga keamana aset informasi yang dimiliki oleh STIE Perbanas.
3. Memberikan kontribusi mengenai penyusunan dokumen SOP *(Standard Operating Procedure)* terkait dengan kendali akses yang mengacu pada kerangka kerja ISO/IEC 27002:2013.
4. Dokumen SOP *(Standard Operating Procedure)* yang dihasilkan dapat digunakan sebagai panduan atau langkah dasar untuk melakukan pengelolaan terhadap kendali akses.

1.6 Relevansi

Topik yang diangkat pada tugas akhir ini adalah mengenai Pembuatan SOP *(Standard Operating Procedure)* Keamanan Aset Informasi Berdasarkan Kendali Akses Dengan Menggunakan ISO/IEC:27002:2013 Pada Studi Kasus Perbanas. Topik ini ada kaitannya dengan Manajemen Sistem Informasi serta Tata Kelola pada kerangka penelitian Manajemen Sistem Informasi (MSI), topik yang diangkat dalam tugas akhir ini ada kaitannya dengan mata kuliah Tata Kelola TI dan Manajemen Risiko TI.

(Halaman ini sengaja dikosongkan)

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Dalam mengerjakan tugas akhir ini terdapat beberapa penelitian serupa yang telah dilakukan yang digunakan sebagai referensi, berikut ini adalah informasi singkat mengenai penelitian-penelitian serupa yang sudah dilakukan sebelum penelitian ini.

Tabel 2. 1 Penelitian Sebelumnya

Judul : Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I	
Nama Peneliti	Margo Utomo, Ahmad Holil Noor Ali, Irsal Affandi
Tahun Penelitian	2012
Hasil Penelitian	Hasil dari penelitian yang dilakukan ini adalah berupa dokumen tata kelola teknologi informasi yang terdiri dari dokumen manual, dokumen prosedur, instruksi kerja dan formulir yang berhubungan keamanan informasi kontrol akses. Kontrol yang didapatkan adalah ditentukan berdasarkan hasil penilaian risiko pada aset informasi yang paling tinggi.
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah terletak pada metodologi penelitiannya dimana penentuan kontrol dari standard maupun kerangka kerja dipetakan terlebih

	dahulu berdasarkan pada hasil penghitungan risiko yang memiliki nilai paling tinggi.
Judul : Pembuatan Dokumen SOP (Standard Operating Procedure) Keamanan Data Yang Mengacu Pada Kontrol Kerangka Kerja Cobit 5 Dan ISO 27002:2013 (Studi Kasus : STIE Perbanas)	
Nama Peneliti	Aulia Nur Fatimah
Tahun Penelitian	2015
Hasil Penelitian	Hasil dari penelitian yang dilakukan ini adalah berupa dokumen prosedur mengenai keamanan data, formulir yang berhubungan dengan keamanan data, instruksi kerja, dan juga terdapat rekomendasi mitigasi risiko yang sebaiknya dilakukan. Kontrol yang dilakukan ditentukan berdasarkan hasil penilaian risiko pada aset informasi yang paling tinggi.
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah objek penelitian memiliki kesamaan yaitu di STIE Perbanas dan juga memiliki metodologi penelitian yang penentuan kontrolnya dilakukan berdasarkan pemetaan kerangka kerja terlebih dahulu berdasarkan pada hasil penilaian risiko yang memiliki nilai paling tinggi.

2.2 Dasar Teori

Dasar teori merupakan penjelasan mengenai teori-teori yang digunakan untuk mendukung pengerjaan tugas akhir. Terdapat beberapa teori yang digunakan dalam pengerjaan tugas akhir ini diantaranya adalah Aset, Aset Informasi, Keamanan Informasi, Kendali Akses, ISO/IEC:27002:2013, Komponen SI/TI, Risiko, Risiko Teknologi Informasi, Manajemen Risiko, Manajemen Risiko Teknologi Informasi, FMEA *(Failure Modes and Effects Analysis)),* OCTAVE *(Operationally Critical Threat, Asset and Vulnerability),* SOP *(Standard Operating Procedure)* dan Format dokumen SOP *(Standard Operating Procedure*.

2.2.1 Aset

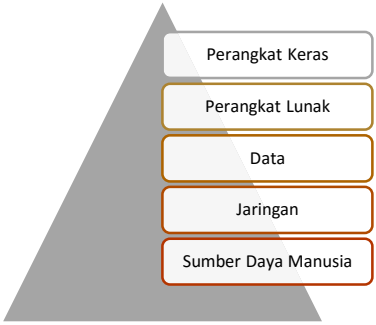
Terdapat beberapa definisi mengenai Aset menurut beberapa sumber antara lain :

- Menurut FSAC No.6 prg 25 mendefinisikan aset sebagai manfaat ekonomi masa datang yang cukup pasti atau diperoleh atau dikuasai atau dikendalikan oleh suatu entitas akibat transaksi atau kejadian masa lalu.
- Menurut International Accounting Standard Committee (IASC) mendifinisikan aset adalah sebagai sumber daya yang dikendalikan oleh suatu entitas sebagai hasil kejadian masa lalu yang mana manfaat ekonomis masa depan diharapkan didapatkan oleh perusahaan.
- Sedangkan Kerangka Konseptual Akuntansi Pemerintah (Lampiran II PP No 24 tahun 2005) mendefinisikan asset lebih luas lagi, yaitu sebagai sumber daya ekonomi yang dikuasai dan atau dimiliki oleh suatu pemerintah sebagai akibat dari peristiwa masa lalu dan daripadanya diperoleh manfaat ekonomi baik oleh pemerintah maupun oleh masyarakat, dan dapat diukur dalam satuan uang, termasuk sumber daya non keuangan yang

diperlukan untuk penyediaan jasa bagi masyarakat umum dan sumber daya yang dipelihara karena alasan sejarah dan budaya.

2.2.2 Aset Informasi

Menurut A.Rohmani (2014) mendefinisikan aset informasi adalah sesuatu yang terdefinisi dan terkelola sebagai satu unit informasi sehingga dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif. Dalam arti lain bisa juga didefinisikan sebagai sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti tanpa biaya, keahlian, waktu, sumber daya dan kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi. Aset informasi pada penelitian ini akan mengacu pada definisi Sistem Informasi. Komponen sistem informasi dibangun berdasarkan komponen-komponen pendukung yang meliputi : sumber daya manusia *(people)*, perangkat keras *(hardware)*, perangkat lunak *(software)*, dan data dan jaringan *(network)*. Dimana kelima komponen tersebut saling menyatu dan berinteraksi sehingga dapat berfungsi sebagai pendukung dan *enabler* dalam meningkatkan operasi keseharian bisnis, serta penyedia kebutuhan informasi dalam rangka pengambilan keputusan yang baik.



Gambar 2. 1 Komponen Aset Informasi

Pada gambar diatas diibaratkan sebuah sistem informasi yang terdiri dari beberapa komponen penyusunnya. Komponen tersebut yaitu sebagai berikut :

a. Perangkat Keras *(Hardware)*
   Perangkat keras mencakup piranti fisik seperti : komputer, printer, monitor dan server. Berperan penting sebagai media penyimpanan vital dalam dunia sistem informasi. Dimana setiap perusahaan yang memiliki teknologi informasi memiliki *hardware* yang komplek dan berjumlah banyak.
b. Perangkat Lunak *(Software)*
   Perangkat lunak merupakan sekumpulan instruksi yang dapat mempengaruhi kinerja perangkat keras dan memproses data. Tujuan adanya ini adalah untuk mengolah, menghitung dan memanipulasi data agar menghasilkan informasi yang berguna.
c. Data
   Data dalam dunia teknologi informasi adalah sebuah bagian dari database, yang disimpan dalam basis data sebagai penyedia informasi dalam tujuannya untuk mendukung perusahaan melakukan kegiatan operasional.
d. Jaringan *(Network)*
   Jaringan merupakan sebuah sistem penghubung yang memungkinkan suatu sumber (utamanya perangkat keras dan perangkat lunak) digunakan secara bersamaan dalam waktu yang berbeda.
e. Sumber Daya Manusia *(People)*
   Sumber daya manusia atau orang dalam penelitian ini adalah civitas akademika dalam STIE Perbanas baik dalam bagian teknologi informasi maupun non teknologi informasi dan yang berhubungan dengan sistem informasi maupun tidak. Sumber daya manusia tersebut antara lain staf teknologi

informasi dan non teknologi informasi serta Dosen dan Mahasiswa.

2.2.3 Keamanan Informasi

Menurut Sarno dan Iffano (2009) keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoptimalkan pengembalian investasi *(return on investment)*. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di *share* maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sarno dan Iffano, 2009). Keamanan informasi memiliki keterkaitan dengan perlindungan aset berharga terhadap kehilangan, penyalahgunaan, atau kerusakan. Aset berharga disini adalah informasi yang direkam, diproses, disimpan, dikirim atau diambil baik dari media elektronik ataupun non elektronik. Perlindungan aset diperlukan untuk melakukan tindakan menjaga informasi dari seluruh ancaman yang dapat terjadi serta memastikan bahwa kelangsungan bisnis akan tetap terjadi dengan risiko yang semakin minimal.

Keamanan informasi memiliki tiga aspek, ketiga aspek tersebut bisa disebut dengan CIA Triad Model yaitu [1]:

1. ***Confidentiality***

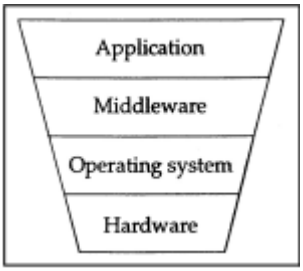
   Keamanan informasi menjamin bahwa hanya orang tertentu yang memiliki hak akses yang akan diperbolehkan untuk mengakses informasi tersebut

serta pencegahan dari orang yang tidak berhak untuk mengakses.

2. ***Integrity***
   Keamanan informasi menjamin kelengkapan dan keakuratan dari informasi yang akan diberikan serta memastikan bahwa informasi tersebut belum dimodifikasi oleh pihak yang tidak berhak.
3. ***Availability***
   Keamanan informasi menjamin pengguna memiliki kesempatan yang sama dalam melakukan akses pada suatu informasi.

2.2.3 Kendali Akses

Kendali Akses merupakan pusat keamanan sistem. Kendali akses merupakan sebuah kendali yang berfungsi untuk mengontrol pengguna (Orang, proses, mesin, dll) yang memiliki akses terhadap sumber daya yang ada di dalam sistem yang mana akses tersebut bias digunakan untuk membaca, memprogram dan kemudian dilakukan eksekusi, dan juga bias berbagi data dengan pengguna yang lain. (Ross Anderson)



Gambar 2. 2 Level kendali akses dalam sebuah sistem

Kendali akses memiliki tingkatan seperti ditunjukan pada Gambar 1, berikut ini adalah deskripsi dari masing-masing level:

- *Mekanisme kendali akses yang dapat dilihat oleh pengguna pada level aplikasi memiliki kebijakan keamanan yang sangat ketat dan komplek*. Sebagai contoh sebuah bisnis online yang modern bisa menugaskan satu staff namun memiliki peran yang berbeda beda, yang mana dalam satu tugas bisa mengandung beberapa transaksi penting yang ada dalam sistem. Misalkan seperti transaksi kartu kredit dengan pelanggan, hal tersebut memerlukan otoritas online dari pihak ketiga sehingga membutuhkan dual kontrol.
- *Aplikasi dapat ditulis di atas middleware, seperti database sistem manajemen atau paket pembukuan yang memaksa sistem harus diberi perlindungan khusus.* Misalnya, perangkat lunak pembukuan dapat memastikan bahwa transaksi pada debet harus memiliki jumlah yang sama terhadap transaksi kredit yang ada di pembukuan.
- *Middleware akan menggunakan fasilitas yang disediakan oleh sistem operasi yang mendasarinya.* Karena pada level ini membangun sumber daya seperti file dan port komunikasi dari tingkat komponen yang lebih rendah, maka hal tersebut membutuhkan tanggung jawab untuk menyediakan cara untuk mengendalikan akses kepada mereka.
- *Dan yang terakhir, sistem operasi kendali akses biasanya akan bergantung pada fitur perangkat keras yang disediakan oleh prosesor atau dengan manajemen memori yang dimiliki oleh perangkat keras tersebut.* Kontrol ini yang menyimpan

history siapa saja yang melakukan akses terhadap sistem.

Adapun prinsip-prinsip dari kendali akses menurut Saltzer dan Schroeder 75, diantaranya adalah sebagai berikut :

1. *Economy of mechanism*
   - Tetap menjaga agar desain dibuat sesimpel dan sekeceil mungkin.
2. *Fail-safe defaults*
   - Defaultnya adalah tidak ada akses
3. *Complete mediation*
   - Setiap akses yang dilakukan harus diperiksa
4. *Open design*
   - Keamanan tidak tergantung pada kerahasiaan mekanisme
5. *Separation privilege*
   - Sebuah sistem yang membutuhkan dua kunci memiliki keamanan yang lebih kuat dibandingkan dengan yang hanya membutuhkan satu kunci
6. *Least privilege*
   - Setiap program dan setiap penggunanya harus beroperasi menggunakan hak masing-masing untuk menyelesaikan pekerjaannya
7. *Least common mechanism*
   - "meminimalkan jumlah mekanisme umum untuk lebih dari satu pengguna dan yang tergantung oleh semua pengguna"
8. *Physchological acceptability*
   - "Desain dari interface pengguna harus mudah untuk digunakan"

- Harapan pengguna terhadap tujuan dibuatnya perlindungan harus sesuai dengan mekanisme

2.2.4 ISO/IEC:27002:2013

ISO27002:2013 merupakan standard mengenai keamanan informasi yang dikeluarkan oleh International Organization for Standardization (ISO) dan International Electronical Commision (IEC). ISO 27002 memiliki keterkaitan dengan ISO 27001, dimana dalam dokumen ISO 27001 berisikan kebutuhan mandatory dari sistem manajemen keamanan informasi sedangkan ISO 27002 melengkapinya dengan *code of practice* atau kontrol keamanan informasi untuk risiko keamanan pada kerahasian, keutuhan dan ketersediaan informasi. ISO 27002 memberikan *best practice* bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi (IT Governance Institute & Office of Government Commerce, 2008). ISO/IEC 27002 memiliki 11 klausul utama kontrol yang masing masingnya terdiri dari kategori utama keamanan (*main security categories*) dan kontrol . Kategori utama keamanan terdiri dari 14 area berdasarkan ISO27002:2013 yaitu :

a) *Security Policy* (Kebijakan Keamanan)
b) *Organizing Information Security* (Keamanan Informasi Organisasi)
c) *Human Resources Security* (Keamanan Sumber Daya Manusia)
d) *Asset Management* (Pengelolaan Aset)
e) *Access Control* (Kontrol Akses)
f) *Cryptography* (Kriptografi)
g) *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan)
h) *Operations Security* (Keamanan Operasional)

i) *Communication Security* (Keamanan Komunikasi)
j) *System Acquisition, Development and Maintenance* (Akuisisi, Pengembangan dan Pengelolaan Sistem)
k) *Supplier Relationship* (Hubungan dengan *Supplier*)
l) *Information Security Incident Management* (Pengelolaan Insiden Keamanan Informasi)
m) *Information Security Aspects of Business Continuity Management* (Keamanan Informasi dari Aspek Pengelolaan Keberlangsungan Bisnis) *Compliance* (Kepatuhan)

2.2.5 Risiko

Definisi risiko menurut Kamus Besar Bahasa Indonesia (KBBI) adalah akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Menurut Arthur J. Keown (2000), risiko adalah prospek suatu hasil yang tidak disukan (operasional sebagai deviasi standar).

Sedangkan definisi risiko menurut Hanafi (2006) adalah risiko merupakan besarnya penyimpangan antara tingkat pengembalian yang diharapkan (*expected return*-ER) dengan tingkat pengembalian aktual (*actual return).* Terdapat definisi lain lagi menurut Emmaett J. Vaughan dan Curtis M. Elliott (1978), risiko didefinisikan sebagai:

a. Kans kerugian – *the chance of loss*
b. Kemungkinan kerugian – *possibility of loss*
c. Ketidakpastian – *uncertainty*
d. Penyimpangan kenyataan dari hasil yang diharapkan – *the dispersion of actual from expected result*

e. Probabilitas bahwa suatu hasil berbeda dari yang diharapkan – *the probability of any outcome different from the one expected*

2.2.6 Risiko Teknologi Informasi

Tidak bisa dipungkiri bahwa di era sekarang penggunaan teknologi informasi semakin meningkat dikarenakan kebutuhan akan teknologi yang semakin besar pula. Dengan semakin meningkatnya penggunaan teknologi informasi ini menyebabkan ketergantungan organisasi maupun perusahaan teknologi informasi semakin besar, hal ini menyebabkan pula risiko teknologi informasi yang semakin meningkat karena ketergantungan organisasi maupun perusahaan tersebut. Menurut George & Hunter (2007) risiko teknologi informasi adalah sebeuah kejadian yang tidak dapat direncanakan dan berdampak pada kegagalan atau penyalahgunaan teknologi informasi yang mengancam tujuan bisnis.

Sedangkan menurut Hughes (2006, p36), dalam penggunaan teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya yang tercakup dalam 6 kategori, yaitu :

a. Keamanan
   Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berwenang. Misalnya saja kejahatan komputer, kebocoran internal dan terorisme *cyber*.
b. Ketersediaan
   Risiko yang datanya tidak dapat diakses setelah kegagalan sistem, karena kesalahan manusia (*human error*), perubahan konfigurasi, dan kurangnya penggunaan arsitektur yang benar.
c. Daya Pulih
   Risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah

terjadinya kegagalan dalam perangkat lunak atau perangkat keras, ancaman *eksternal*, atau bencana alam.

d. Performa
   Risiko dimana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi dan topografi informasi teknologi informasi yang beragam.
e. Daya Skala
   Risiko yang perkembangan bisnis, pengaturan *bottleneck*, dam bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.
f. Ketaatan
   Risiko yang manajemen atau penggunaan informasinya melanggar keperluan dari pihak pengatur. Yang dipersalahkan dalam hal ini mencakup aturan pemerintah, panduan pengaturan perusahaan dan kebijakan internal.

2.2.7 Manajemen Risiko

Menurut *Institute of Risk Management* (IRM) manajemen risiko sebagai suatu proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi dan mengambil tindakan untuk risiko-risiko yang muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan. Dan menurut Djohantoputro dalam penelitiannya *Manajemen Risiko Korporat* dikatakan bahwa manajemen risiko merupakan suatu proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternative penanganan risiko dan monitor serta pengendalian penanganan risiko (Djohanputro, 2008). Sehingga dapat disimpulkan bahwa manajemen risiko adalah sebuah proses yang di dalamnya terdapat aktifitas pengelolaan risiko untuk

meminimalisir kerugian atau dampak bagi organisasi atau perusahaan.

2.2.8 Manajemen Risiko Teknologi Informasi

Menurut Jones, Federick & Rama (2008, p.193), manajemen risiko adalah kegiatan pemimpin puncak mengidentifikasi, menangani, dan memonitor risiko bisnis yang dihadapi perusahaan mereka di masa yang akan datang. Menurut Blokdjik (2008, p82), manajemen risiko ini memiliki tugas tersendiri yaitu mengelola risiko suatu proyek. Tujuan dari dikelolanya risiko tersebut adalah untuk menjaga hubungan ke tingkat yang dapat diterima dengan cara yang hemat biaya. Manajemen risiko sendiri meliputi: akses yang dapat dipercaya, tentang risiko yang terbaru, proses pengambilan keputusan didukung oleh kerangka analisis risiko dan proses evaluasi, memantau risiko, pengendalian yang tepat untuk menghadapi risiko.

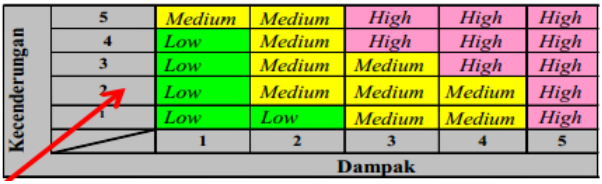
Dalam manajemen risiko teknologi informasi pada umumnya akan diikuti dengan penentuan risiko mana yang membawa pengaruh atau dampak yang bisa menyebabkan kerugian bagi organisasi maupun perusahaan, mulai dari dampak yang paling besar sampai kecil dan risiko mana yang akan ditangani terlebih dahulu. Langkah-langkah penanganan risiko potensial yang dapat diambil oleh organisasi maupun perusahaan adalah sebagai berikut :

a. Accept

Manajemen memutuskan untuk menerima risiko jika besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi organisasi.

Contohnya adalah

1. Dengan menetapkan Kriteria Penerimaan Risiko terkait dengan evaluasi dan penanganan risiko misalnya Nilai Akhir Risiko "*Low*".



Gambar 2. 3 Contoh nilai risiko

2. Nilai Akhir Risiko "*Medium*" atau "*High*", namun telah diputuskan untuk diterima oleh manajemen dan dibuat suatu sistem prosedur untuk memantau risiko tersebut misalnya dengan menyediakan tambahan modal sesuai besarnya potensi risiko.

b. Avoid

Organisasi memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan output yang sama untuk menghindari terjadinya risiko.

Contohnya hak *privilege administrator* pada *user* yang menggunakan PC yang mengandung risiko akan adanya *malicious code* pada PC. Risiko ini dapat dihindari dengan tidak memberikan hak *privilege* pada *user* sehinggan *user* tidak bisa merubah konfigurasi dan meng-*install software* pada PC.

c. Mitigate

Organisasi memutuskan untuk mengurangi dampak maupun kemungkinan terjadinya risiko.

Contohnya penggunaan PC untuk mendukung proses bisnis organisasi mengandung risiok terjadinya *hacking* pada PC. Pengendalian risiko dilakukan dengan pemasangan fasilitas *firewall* untuk mencegah akses yang tidak terotorisasi.

d. Transfer

Organisasi memutuskan untuk mengalihkan seluruh atau sebagian tanggun jawab pelaksanaan suatu proses kepada pihak ketiga.

Contohnya penggunaan fasilitas ruangan atau gedung mengandung risiko terjadi kebakaran. Risiko ini ditangan dengan memindahkan risiko ke perusahaan asuransi yaitu dengan mengasuransikan fasilitas ruangan atau gedung.

2.2.9 FMEA *(Failure Modes and Effects Analysis)*

FMEA merupakan suatu prosedur terstruktur untuk mengidentifikasi dan mencegah sebanyak mungkin mode kegagalan *(failure mode)*. FMEA digunakan untuk mengidentifikasi sumber-sumber dan akar penyebab dari suatu masalah kualitas. Suatu mode kegagalan adalah apa saja yang termasuk dalam kecacatan/kegagalan dalam desain, kondisi diluar batas spesifikasi yang telah ditentukan maupun perubahan dalam produk yang menyebabkan terganggunya fungsi dari produk tersebut. Para ahli memiliki beberapa definisi mengenai FMEA *(failure modes and effect analysis)*, definisi tersebut memiliki arti yang cukup luas dan apabila dievaluasi lebih dalam memiliki arti yang serupa. Definisi FMEA *(failure modes and effect analysis)* tersebut disampaikan oleh *Roger D. Leitch* bahwa definisi dari FMEA adalah analisa teknik yang apabila dilakukan dengan tepat dan waktu yang tepat pula akan memberikan nilai yang besar dalam membantu proses pembuatan keputusan. Analisa tersebut biasa disebut dengan analisa *"bottom up"*, seperti dilakukan pemeriksaan pada proses produksi tingkat awal dan mempertimbangkan kegagalan sistem yang merupakan hasil dari keseluruhan bentuk kegagalan yang berbeda.

Terdapat juga langkah langkah dalam melakukan FMEA, berikut ini adalah langkah-langkah dalam melakukan FMEA :

1. Mengidentifikasi komponen-komponen dan fungsi yang terkait

2. Mengidentifikasi mode kegagalan *(failure modes)*
3. Mengidentifikasi dampak dari mode kegagalan *(failure mode)*
4. Menentukan nilai keparahan *(severity)* dari kegagalan
5. Mengidentifikasi penyebab dari kegagalan
6. Menentukan nilai frekuensi sering terjadinya kegagalan *(occurrence)*
7. Mengidentifikasi kontrol yang diperlukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan *(detection)*
9. Melakukan kalkulasi nilai RPN *(risk priority number)*
10. Menentukan tindakan untuk mengurangi kegagalan.

Pada penelitian ini penentuan kontrol yang dibutuhkan dalam penyusunan SOP tersebut akan berdasarkan pada kebutuhan kendali akses yang kritis dilihat dari segi analisisi nilai atau level risiko yang memiliki kategori prioritas *very high* dan *high* dalam aspek operasional.

2.2.10 OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability)*

OCTAVE merupakan sebuah *framework* yang ditujukan untuk melakukan manajemen risiko terkait dengan keamanan aset organisasi. Octave membuat pendekatan standarisasi untuk mengedalikan risiko dan *practice based* untuk evaluasi keamanan informasi. Octave ini digunakan untuk mengidentifikasi dan mengatur risiko keamanan informasi. Dalam melakukan manajemen risiko, Octave menggunakan metode evaluasi secara komprehensif yang memungkinkan organisasi untuk mengidentifikasi aset informasi yang penting untuk misi pada perusahaan (Christoper J.Albertrs, 1999).

Gambar 2. 4 Framework Octave

Octave menggunakan pendekatan tiga tahapan dalam menguji isu organisasi terhadap penysunan masalah yang komprehensif dan berhubungan dengan kebutuhan keamanan sebuah organisasi. Berikut merupakan penjelasan dari masing-masing tahap yang ada dalam Octave :

- Tahap 1 : Membangun Aset Berbasis Ancaman Profil

  Tahapan ini merupakan bagian dari *organizational view* yang melihat dari sisi internal organisasi, sehingga luaran dari tahapan ini adalah aset penting organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan organisasi dan kelemahan kebijakan yang dimiliki organisasi saat ini.

- Tahap 2 : Idenfitikasi Infrastruktur *Vulnerabilities*

  Tahapan ini akan melihat dari sisi teknologi yaitu melakukan evaluasi terhadap infrastruktur teknologi informasi yang dimiliki organisasi. Sehingga luaran dari tahapan ini adalah berupa komponen penting dalam aset kritis dan kelemahan

infrasatruktur teknologi informasi yang ada saat ini.

- Tahap 3 : Mengembangkan Strategi Keamanan dan Perencanaan
  Tahapan ini merupakan tahapan penilaian risiko dan mitigasi risiko dengan melakukan pengembangan strategi keamanan dan perencanaannya. Sehingga luaran yang dihasilkan dari tahapan ini adalah berupa analisisi risiko, pengukuruan tingkat risiko dan strategi proteksi.

2.2.11 SOP (Standard Operating Procedure)

Pada setiap organisasi maupun perusahaan pasti memiliki serangkaian proses pada tiap pekerjaan. Proses ini harus dirancang dan dikembangkan dengan baik. Hal tersebut dilakukan untuk menghindari kesalahan selama pekerjaan tersebut dilaksanakan. Sehingga untuk menghindari hal tersebut perlu dibuat suatu prosedur untuk menciptakan standarisasi suatu pekerjaan sehingga siapapun yang melakukan pekerjaan tersebut langkahnya tidak berubah ubah. Prosedur inilah yang disebut dengan *Standard Operating Procedure* atau biasa disingkat dengan SOP.

SOP sendiri memiliki beberapa peangertian, menurut Istyadi Insani dalam bukunya yang berjudul Standar Operasional Prosedur (SOP) sebagai pedoman pelaksanaan administrasi perkantoran dalam rangka peningkatan pelayanan. Pengertian lain dijelaskan pada buku United States Environmental Protection Agency yang menyatakan bahwa pada hakekatnya SOP berarti suatu cara untuk menghindari miskomunikasi, konflik dan permasalahan pada pelaksanaan tugas/pekerjaan pada suatu organisasi. Definisi lain dijelaskan oleh Gareth R. Jones dalam bukunya Organiszational Theory, yang menyatakan bahwa SOP merupakan

bagian dari peraturan tertulis yang membantu untuk mengontrol perilaku anggota organisasi. Menurut Tjipto Atmoko, *Standard Operational Procedure* (SOP) merupakan suatu pedoman atau acuan untuk melaksanakan tugas pekerjaan sesuai dengan fungsi dan alat penialian kinerja instansi pemerintah berdasarkan indikator-indikator teknis, administrative dan prosedural sesuai tata kerja, prosedur kerja dan sistem kerja pada unit kerja yang bersangkutan.

Tjipto Atmoko pun menyebutkan bahwa dalam membuat *Standard Operating Procedure* (SOP) terdapat prinsip-prinsip yang harus diterapkan dalam melakukan penyusunannya, berikut ini adalah prinsip-prinsip penyusunan *Standard Operating Procedure* (SOP) :

- *Standard Operating Procedure* (SOP) harus ditulis secara jelas, sederhana dan tidak berbelit belit sehingga mudah dimengerti dan diterapkan untuk satu kegiatan tertentu.
- *Standard Operating Procedure* (SOP) harus dapat menjadi pedoman yang terukur baik mengenai norma waktu, hasil kerja yang tepat dan akurat, maupun rincian biaya pelayanan dan tata cara pembayaran bila diperlukan adanya biaya pelayanan.
- *Standard Operating Procedure* (SOP) harus dapat memberikan kejelasan kapan dan siapa yang harus melaksanakan kegiatan, berapa lama waktu yang dibutuhkan dan sampai dimana tanggung jawab masing-masing pegawai/pejabat.
- *Standard Operating Procedure* (SOP) harus sudah dirumuskan dan selalu bisa menyesuaikan dengan kebutuhan dan perkembangan kebijakan yang berlaku.

- *Standard Operating Procedure* (SOP) harus menggambarkan alur kegiatan yang mudah ditelusuri jika terjadi hambatan.

2.2.12 Format Dokumen SOP

Menurut Tjipto Atmoko, terdapat beberapa jenis format dalam pembuatan SOP, yang pertama adalah Langkah sederhana (simple steps), yang kedua adalah Tahapan berurutan (Hierarchical steps), yang ketiga adalah Grafik (graphic), dan yang terakhir adalah Diagram alir (flowcharts). Terdapat empat faktor yang dapat dijadikan dasar dalam penentuan format penyusunan Standard Operating Procedure (SOP) yang akan dipakai oleh suatu organisasi yaitu :

- Banyaknya keputusan yang akan dibuat dalam suatu prosedur.
- Banyaknya langkah dan sub langkah yang diperlukan dalam suatu prosedur.
- Siapa yang akan dijadikan target sebagai pelaksana Standard Operating Procedure (SOP).
- Tujuan yang ingin dicapai dalam pembuatan Standard Operating Procedure (SOP) ini.

Ada 4 jenis format umum Standard Operating Procedure (SOP), diantaranya adalah sebagai berikut :

a. Langkah sederhana (simple steps)
   Simple steps dapat digunakan jika prosedur yang akan disusun hanya memuat sedikit kegiatan dan memerlukan sedikit keputusan yang bersifat sederhana. Format SOP ini dapat digunakan dalam situasi dimana hanya ada beberapa orang yang akan melaksanakan prosedur yang telah disusun.
b. Tahapan berurutan (Hierarchical steps)
   Format ini merupakan pengembangan dari simple steps. Digunakan jika prosedur yang disusun panjang, lebih dari 10 langkah dan membutuhkan

informasi yang lebih detail, akan tetapi hanya memerlukan sedikit pengambilan keputusan.

c. Grafik (graphic)
   Format grafik ini bertujuan untuk memudahkan dalam memahami prosedur yang ada dan biasanya ditujukan untuk pelaksanaan eksternal organisasi (pemohon).
d. Diagram alir (flowcharts)
   Flowcharts merupakan format yang biasa digunakan, jika dalam Standard Operating Procedure (SOP) diperlukan pengambilan keputusan yang banyak (kompleks) dan membutuhkan opsi jawaban (alternative jawaban) seperti : jawaban "ya" atau "tidak", "lengkap" atau "tidak", "benar" atau "salah", dsb. Simbol-simbol tersebut memiliki fungsi yang bersifat khas (teknis dan khusus) yang pada dasarnya dikembangkan dari simbol dasar flowcharts (basic symbols of flowcharts) yang terdiri dari 4 simbol, yaitu:
   1. Simbol kapsul/terminator, untuk mendeskripsikan kegiatan mulai dan berakhir.
   2. Simbol kotak/process, untuk mendeskripsikan proses atau kegiatan eksekusi.
   3. Simbol belah ketupat/decision, untuk mendeskripsikan kegiatan pengambilan keputusan.
   4. Simbol anak panah/arrow, untuk mendeskripsikan arah kegiatan (alur proses kegiatan).
   5. Simbol segi lima/off-page connector, untuk mendeskripsikan hubungan antar simbol yang berbeda halaman.

Format *Standard Operating Procedure* (SOP) dalam bentuk flowcharts terdiri dari 2 jenis yaitu :

1. Linear flowcharts (diagram alir linier)

Ciri utama dari format linear flowcharts ini adalah unsur kegiatan yang disatukan, yaitu : unsur kegiatan atau unsur pelaksanaannya dan menuliskan rumusan kegiatan secara singkat didalam simbol yang dipakai.

2. Branching flowcharts (diagram alir bercabang)
   Format Branching Flowcharts memiliki ciri utama dipisahkannya unsur pelaksana dalam kolom-kolom yang terpisah dari kolom kegiatan dan menggambarkan prosedur kegiatan dalam bentuk simbol yang dihubungkan secara bercabang-cabang.

Format penyusunan dokumen SOP ini akan digunakan untuk memudahkan dalam menyusun SOP dan juga sebagai acuan pembuatan dokumen SOP kendali akses pada STIE Perbanas. Berikut ini format umum penyusunan dokumen SOP yang harus memenuhi unsur dokumentasi dan usur prosedur.

1. Unsur Dokumentasi

Unsur dokumentasi merupakan unsur yang terkait dengan proses pendokumentasian SOP sebagai sebuah dokumen. Unsur dokumentasi yaitu halaman judul, keputusan pimpinan terkait, dan deskripsi singkat penggunaan dokumen.

a) Halaman Judul *(Cover)*

Halaman judul merupakan halaman yang menjadi sampul dari dokumen SOP dan harus mampu memberikan informasi mengenai isi dokumen. Sehingga dalam halaman judul beberapa hal yang harus ada adalah judul SOP, instansi/satuan kerja, tahun pembuatan dan keterangan informasi lain sesuai persetujuan organisasi terkait.

b) Daftar Isi Dokumen SOP

Daftar isi digunakan untuk mempercepat pencarian informasi dan menulis perubahan atau revisi dari bagian tertentu pada SOP.

c) Deskripsi Penggunaan Dokumen

Dalam diskripsi singkat penggunaan dokumen, perlu dijelaskan mengenai ruang lingkup yang membahas mengenai tujuan disusunnya prosedur, ringkasan mengenai prosedur yang disusun dan definisi kata yang terkait di dalam dokumen SOP.

2. Unsur Prosedur

Unsur prosedur merupakan bagian identitas dan bagian alur prosedur atau *flowchart.* Berikut adalah masing-masing penjelasannya.

a) Bagian Identitas

Bagian identitas dalam dokumen SOP berisikan logo dan nama instansi terkait, nomor SOP, tanggal pembuatan, tanggal revisi, tanggal efektif, pengesahan dokumen, judul SOP, dasar hukum dan identitas lainnya sesuai dengan kebijakan dan persetujuan organisasi terkait.

KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI
DEPUTI BIDANG TATALAKSANA
ASISTEN DEPUTI PENGEMBANGAN SISTEM DAN PROSEDUR PEMERINTAHAN

NOMOR SOP	: KPAN/RB/D.IV/4/001/2011
TGL. PEMBUATAN	: 5 Juli 2011
TGL. REVISI	
TGL. EFEKTIF	: 5 Agustus 2011
DISAHKAN OLEH	: Asisten Deputi Pengembangan Sistem dan Prosedur Pemerintahan Nama NIP
NAMA SOP	: PEMBUATAN LAPORAN KONSINYERING

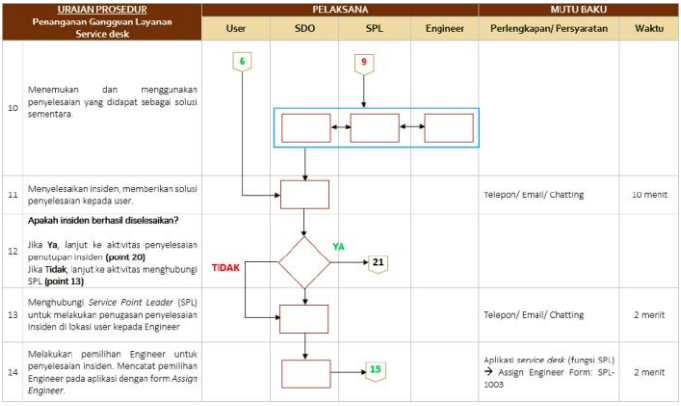
DASAR HUKUM:	KUALIFIKASI PELAKSANA:
1. Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2009 tentang Pembentukan dan Organisasi Kementerian Negara 2. Peraturan Presiden Republik Indonesia Nomor 24 Tahun 2010 tentang Kedudukan, Tugas, dan Fungsi Kementerian Negara serta Susunan Organasi, Tugas, dan Fungsi Eselon I Kementerian Negara 3. Peraturan Menteri Negara PAN dan RB Nomor 12 Tahun 2010 tentang Organisasi Dan Tata Kerja Kementerian PAN dan RB	1. Memiliki kemampuan pengolahan data sederhana 2. Mengetahui tugas dan fungsi Sistem dan Prosedur Pemerintahan 3. Mengetahui tugas dan fungsi mekanisme pembuatan laporan
KETERKAITAN:	**PERALATAN/PERLENGKAPAN:**
1. SOP Pelaksanaan Konsinyering 2. SOP Pendokumentasian Laporan Konsinyering 3. SOP Pencairan Anggaran Konsinyering	1. Lembar Kerja / Rencana Kerja dan Anggaran 2. Term of Reference 3. Komputer/Printer/Scanner 4. Jaringan internet
PERINGATAN:	**PENCATATAN DAN PENDATAAN:**
Apabila Laporan Konsinyering terlambat dibuat maka pelaksanaan kegiatan Konsinyering berikutnya akan tertunda.	- Di simpan sebagai data elektronik dan manual

Gambar 2. 5 Contoh bagian Identitas Prosedur

b) Alur Prosedur

Bagian alur prosedur merupakan bagian yang berisikan penjelasan langkah-langkah prosedur kegiatan beserta mutu baku dan keterangan yang diperlukan. Alur prosedur dibentuk dalam sebuah *flowchart* yang menjelaskan langkah dari kegiatan secara berurutan dan sistematis. Bagan alur atau *flowchart* adalah salah satu unsur dari sebuah prosedur. *Flowchart* merupakan bagian yang berisi penjelasan langkah-langkah sebuah prosedur atau kegiatan beserta standard baku dan keterangan yang diperlukan.

Berikut merupakan contoh bagian *flowchart* yang sistematis dan memenuhi standard isi bagan alur yang terdiri dari nomor kegiatan, uraian kegiatan yang berisi langkah-langkah (prosedur), pelaksanan yang merupakan pelaku kegiatan, mutu baku yang berisi kelengkapan, waktu, output, dan keterangan.



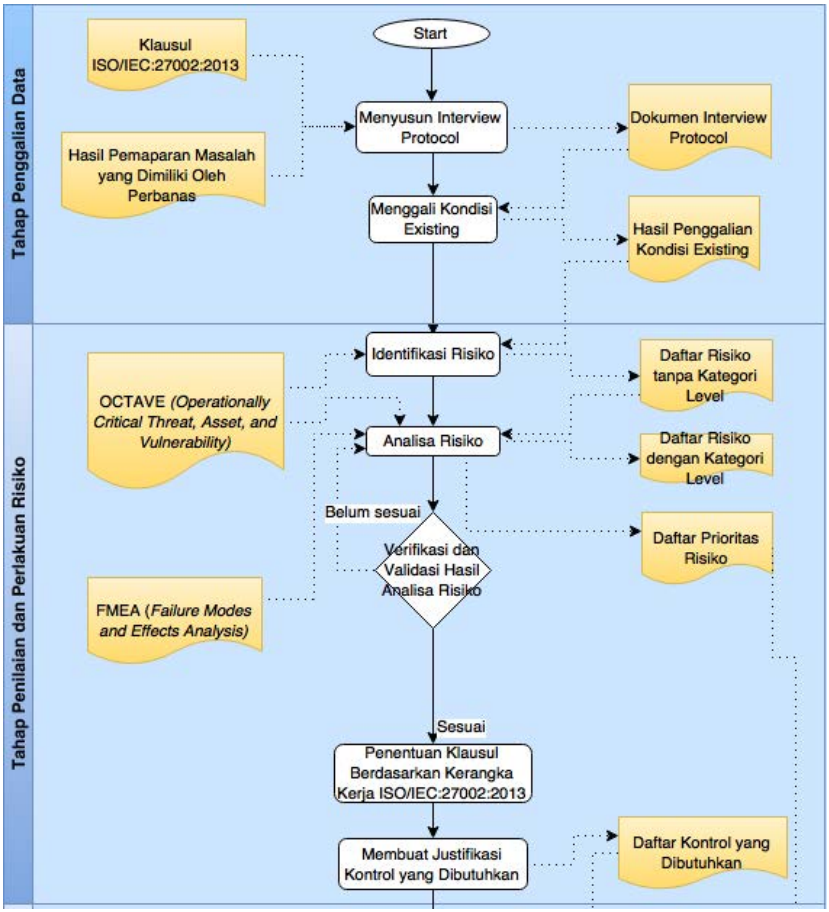
Gambar 2. 6 Contoh Bagan Alur Prosedur

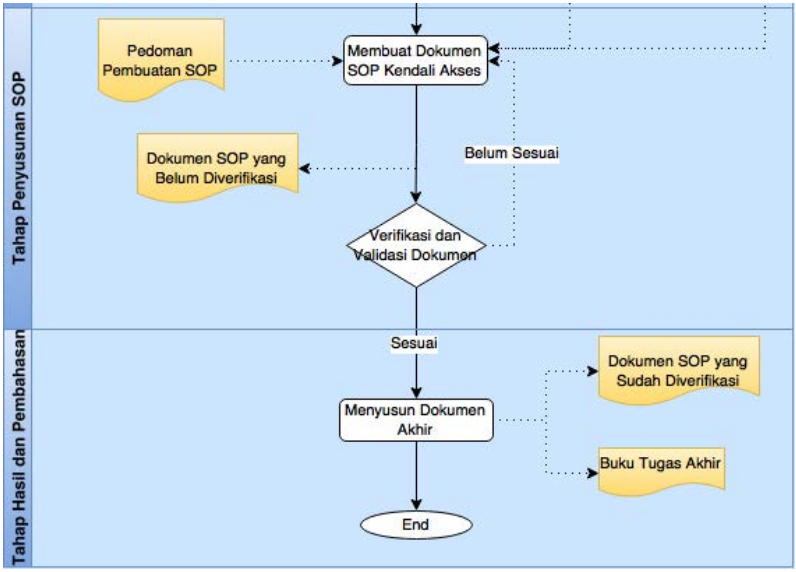
Berdasarkan penjabaran diatas maka dalam penyusunan dokumen SOP terhadap penelitian ini akan digunakan dengan bagan alur untuk menggambarkan alur prosedur yang ada dan

disesuaikan pula berdasarkan kriteria dan struktur atau format yang telah dijelaskan pada subbab sebelumnya. Dokumen SOP yang akan disusun yaitu dokumen SOP untuk kendali akses pada STIE Perbanas yang akan digunakan sebagai prosedur yang telah distandarisasi.

BAB III
METODOLOGI

Diagram metode tugas akhir akan ditampilkan pada gambar dibawah ini :





Gambar 3.1 Metodologi

3.1 Tahap Penggalian Data

Tahap penggalian data adalah tahap awal untuk melakukan penyusunan tugas akhir dan pembuatan produk. Terdapat beberapa proses yang dilakukan pada tahap ini. Pada setiap proses yang dilakukan terdapat input dan outputnya. Proses-proses yang dilakukan pada tahap ini ada 2 yaitu menyusun interview protocol dan menggali kondisi existing. Berikut ini adalah penjelasan dari masing-masing proses pada tahap penggalian data.

3.1.1 Menyusun Interview Protocol

Pada proses menyusun interview protocol ini terdapat dua input yang mempengaruhi dan menjadi pertimbangan dalam melakukan penyusunan interview protocol ini, yang pertama adalah Klausul

ISO/IEC:27002:2013 dan yang kedua adalah hasil pemaparan masalah yang dimiliki oleh Perbanas. Klausul ISO/IEC:27002:2013 ini dijadikan input karena dari kerangka kerja Klausul ISO/IEC:27002:2013 tersebut peneliti bisa mengetahui standard apa saja yang harus ada dalam melakukan pengamanan aset informasi yang ada dalam sebuah organisasi dan kontrol apa saja yang harus dilakukan untuk menjalankan standard tersebut. Dari kerangka kerja tersebut diharapkan bisa terjalin komunikasi lebih lanjut dengan narasumber sehingga bisa menjadi bahan pertimbangan dan disesuaikan dengan kondisi yang ada di STIE Perbanas saat itu. Kemudian input yang kedua adalah hasil catatan dari pemaparan masalah yang dimiliki oleh Perbanas. Pemaparan masalah ini disampaikan langsung oleh Wakil Rektor Pak Didik mengenai kendala apa saja yang dimiliki oleh Perbanas sehingga pihak Perbanas membutuhkan peneliti untuk bisa menindaklanjuti dan membantu memberikan solusi terhadap masalah yang dimiliki oleh STIE Perbanas. Barulah proses penyusunan interview protocol dilakukan berdasarkan dua input tadi. Luaran yang dihasilkan dari proses ini adalah berupa dokumen interview protocol yang nantinya digunakan untuk melakukan interview terhadap narasumber yaitu Ketua SIE TIK (manajemen Jaringan dan Technical Support) untuk bisa menggali informasi yang lebih dalam yang dibutuhkan untuk penelitian ini.

3.1.2 Menggali Kondisi Existing

Pada proses menggali kondisi existing ini input yang dibutuhkan adalah dokumen interview protocol yang sudah dibuat pada proses sebelumnya. Penggalian informasi yang dilakukan pada proses ini adalah penggalian risiko keamanan informasi, contohnya penggalian ditekankan kepada pertanyaan mengenai

kemungkinan risiko operasional yang bisa terjadi dalam STIE Perbanas. Karena hasil dari menggali kondisi existing ini nanti akan digunakan untuk melakukan identifikasi risiko. Selain itu penggalian informasi disini juga ditekankan kepada kendali akses informasi yang ada di STIE Perbanas. Kendali akses ini yang berhubungan pada tiga aspek yaitu kerahasiaan *(confidentiality)*, integritas *(integrity)* dan ketersediaan *(availability)*. Luaran yang dihasilkan dari proses menggali kondisi existing ini adalah berupa hasil wawancara penggalian kondisi existing yang ada di STIE Perbanas.

3.2 Tahap Penilaian dan Perlakuan Risiko

Tahap penilaian dan perlakukan risiko ini didasarkan pada pendekatan *information security risk assessment* pada ISO 27002:2013 yang dibagi dalam lima proses utama yaitu identifikasi risiko, analisa risiko, verifikasi dan validasi hasil risiko, penentuan klausul berdasarkan kerangka kerja ISO/IEC:27002:2013, dan membuat justifikasi kontrol yang dibutuhkan. Masing-masing proses tersebut memiliki input dan output. Berikut ini adalah penjelasan dari masing-masing proses dalam tahap penilaian risiko.

3.2.1 Identifikasi Risiko

Pada proses identifikasi risiko ini terdapat dua input yaitu *framework* Octave dan juga hasil wawancara penggalian kondisi existing yang ada di perbanas. Pada proses ini juga terdapat dua sub proses lagi, yang pertama adalah menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan *(confidentiality),* integritas *(integrity)* dan ketersediaan *(availability)* informasi dalam lingkup sistem manajemen keamanan informasi khususnya pada aspek kendali akses dan yang kedua adalah

mengidentifikasi pemilik risiko. Untuk mendaptkan informasi yang diinginkan terkait dengan hal-hal tersebut, identifikasi risiko akan dilakukan dengan teknik interview kepada pihak manajemen STIE Perbanas. Identifikasi risiko tersebut akan didasarkan pada metode *framework* Octave yaitu dengan melakukan pengidentifikasian terlebih dahulu terhadap aset-aset penting yang dimiliki oleh organisasi, kebutuhan keamanan organisasi, praktek keamanan saat ini yang sudah dilakukan maupun sedang dilakukan, aset-aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Hasil dari identifikasi risiko yang sudah didapatkan tadi kemudian diteruskan ke proses identifikasi pemilik risiko. Luaran yang didapatkan dari proses mengidentifikasi risiko keamanan informasi ini adalah daftar risiko tanpa kategori level. Daftar risiko yang sudah didapatkan akan menjadi pertimbangan dan juga masukan untuk proses analisis risiko.

3.2.2 Analisa Risiko

Pada proses menganalisa risiko ini terdapat tiga input yaitu FMEA *(Failure Modes and Effects Analysis)*, Octave *(Operationally Critical Threat, Asset, and Vulnerability)*, dan daftar risiko. Pada proses ini juga terdapat tiga sub proses lagi yang harus dilakukan, yang pertama adalah menilai potensi yang akan terjadi jika risiko yang telah diidentifikasi tersebut terjadi, yang kedua yaitu menilai kemungkinan terjadinya risiko yang sudah teridentifikasi tersebut dan yang terakhir adalah menentukan level risiko yang sudah diidentifikasi tadi. Analisa risiko tersebut dilakukan dengan menggunakan metode FMEA *(Failure Modes and Effects Analysis)*. Analisis yang akan dilakukan menggunakan metode FMEA ini antara lain mode kegagalan, efek potensial kegagalan, penyebab potensial risiko, dampak potensial risiko,

kemungkinan terjadinya risiko *(Occurrence)*, deteksi *(detection)*, dan nilai level risiko (RPN). Luaran dari proses menganalisis risiko keamanan informasi ini adalah daftar risiko dengan kategori level tiap risiko dan juga daftar prioritas risiko yang nantinya akan diteruskan untuk diverifikasi dan divalidasi oleh pihak STIE Perbanas Surabaya.

3.2.3 Verifikasi dan Validasi Hasil Risiko

Pada proses verifikasi dan validasi hasil risiko ini hal yang dilakukan adalah melakukan verifikasi dan validasi hasil dari evaluasi risiko yang berupa daftar prioritas risiko kepada pihak Manajemen STIE Perbanas. Verifikasi dan validasi ini dilakukan karena untuk meminta pertimabangan dari hasil evaluasi yang telah dilakukan apakah sudah sesuai dan sudah cocok dengan kondisi yang ada di STIE Perbanas saat itu dan apakah prioritas yang diberikan juga sudah sesuai dengan penilaian dari pihak Manajemen STIE Perbanas. Verifikasi dan validasi ini dilakukan secara langsung dengan mempresentasikan hasil daftar prioritas risiko dan revisi juga akan dipaparkan secara langsung pada saat presentasi sehingga revisi langsung dilakukan pada saat presentasi tersebut. Dari verifikasi dan validasi yang dilakukan ini, hasil yang didapatkan adalah daftar prioritas risiko yang sudah diverifikasi dan validasi oleh pihak manajemen STIE Perbanas. Hasil tersebut kemudian akan digunakan untuk menentukan klausul berdasarkan kerangka kerja ISO/IEC:27002:2013 yang terkait dengan kendali akses.

3.2.4 Penentuan Klausul Berdasarkan Kerangka Kerja ISO/IEC:27002:2013

Hal yang dilakukan pada proses penentuan klausul berdasarkan kerangka kerja ISO/IEC:27002:2013 ini adalah menentukan pilihan mitigasi yang sesuai dan

cocok dengan hasil prioritas risiko yang sudah dibuat. Karena fokus dari penelitian yang dilakukan kali ini adalah terkait dengan kendali akses, maka penentuan klausul akan didasarkan pada hasil daftar prioritas risiko yang memiliki kategori Very High dan High yang ada hubungannya dengan kendali akses.

3.2.5 Membuat Justifikasi Kontrol yang Dibutuhkan

Pada proses membuat justifikasi kontrol yang dibutuhkan ini, hal yang dilakukan pada proses ini adalah memilih kontrol yang tepat untuk risiko yang sudah dipilih yang berdasarkan kendali akses. Sehingga penentuan kontrol ini disesuaikan dengan risiko yang ada dan juga memastikan bahwa penentuan dari kontrol yang sudah dipilih ini sesuai dengan mitigasi yang harus dilakukan. Luaran yang dihasilkan dari membuat justifikasi kontrol yang dibutuhkan ini adalah berupa daftar kontrol yang dibutuhkan untuk melakukan mitigasi pada risiko yang ada.

3.3 Tahap Penyusunan SOP

Dalam melakukan penyusunan SOP, terdapat beberapa serangkaian proses yang harus dilakukan diantaranya adalah membuat dokumen SOP kendali akses dan juga verifikasi dan validasi dokumen SOP. Berikut ini merupakan penjelasan dari setiap proses pada tahapan penyusunan SOP.

3.3.1 Membuat Dokumen SOP Kendali Akses

Pada proses membuat dokumen SOP kendali akses ini terdapat dua input yaitu pedoman pembuatan SOP dan juga dafar kontrol yang dibutuhkan untuk melakukan mitigasi terhadap risiko yang ada. Dokumen SOP yang akan dibuat akan disesuaikan dengan konten dokumen yang sudah divalidasi oleh pihak manajemen STIE Perbanas. pembuatan dokumen SOP ini akan

didasarkan pada standard pembuatan dokumen SOP dan juga kontrol yang ada didalamnya merupakan kontrol yang mengacu pada kerangka kerja ISO 27002:2013. Luaran yang dihasilkan pada proses membuat dokumen SOP kendali akses ini adalah dokumen SOP kendali akses yang belum diverifikasi, dokumen tersebut nantinya harus diverifikasi dan validasi terlebih dahulu oleh pihak manajemen STIE Perbanas.

3.3.2 Verifikasi dan Validasi Dokumen

Pada tahapan verifikasi dan validasi dokumen SOP ini input yang dibutuhkan adalah dokumen SOP yang belum. Proses verifikasi dan validasi ini akan dilakukan oleh pihak manajemen STIE Perbanas. Setelah proses verifikasi dan validasi selesai dilakukan dan sudah cocok oleh pihak manajemen STIE Perbanas, proses berikutnya yang dilakukan adalah menyusun dokumen akhir dimana pada proses itulah dokumen akhir dari SOP kendali akses selesai dibuat.

3.4 Tahap Hasil dan Pembahasan

Pada tahap hasil dan pembahasan ini proses akhir yang dilakukan adalah menyusun dokumen akhir. Pada proses menyusun dokumen akhir ini luaran yang dihasilkan ada dua, yang pertama adalah dokumen SOP kendali akses yang sudah diverifikasi dan yang kedua adalah buku tugas akhir. Dokumen SOP kendali akses yang sudah diverifikasi nantinya akan diberikan kepada pihak STIE Perbanas, buku tugas akhir nanti akan digunakan untuk keperluan akademik dan diserahkan ke jurusan sistem informasi. Isi dari dokumen SOP kendali akses nantinya juga akan dimasukkan ke dalam buku tugas akhir untuk memenuhi syarat kelengkapan dalam buku tugas akhir. Buku tugas akhir ini juga bisa diberikan kepada pihak STIE Perbanas jika memang pihak STIE

Perbanas membutuhkan buku tersebut untuk mengetahui bagaimana metode dalam menyusun dokumen SOP kendali akses yang ada di STIE Perbanas.

(halaman ini sengaja dikosongkan)

BAB IV
PERANCANGAN KONSEPTUAL

Bab ini menjelaskan tentang perancangan konseptual dalam mengerjakan tugas akhir ini, yaitu perancangan secara detail dari setiap tahapan pengerjaan yang telah dijelaskan pada metodologi yang ada di Bab III. Dalam tahap perancangan ini, terdapat tiga proses utama yaitu penentuan subjek dan objek penelitian, pembuatan daftar pertanyaan dalam bentuk *interview protocol* untuk wawancara penggalian data dan informasi dan perancangan penilaian risiko serta perancangan SOP.

4.1 Objek Penelitian

Penelitian ini dilakukan pada STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas (Perhimpunan Bank Nasional Swasta) Surabaya yang mana merupakan sebuah lembaga pendidikan tinggi dalam bidang perbankan. Objek yang akan diteliti ada mengenai keamanan aset informasi yang berkaitan dengan kendali akses pada STIE Perbanas. Objek kendali akses pada STIE Perbanas Surabaya ini merupakan salah satu bagian dari keamanan aset informasi yang sedang dikembangkan. dimana dengan terkelolanya kendali akses dengan baik pada STIE Perbanas dapat meningkatkan keefektifan proses bisnis yang berjalan.

Proses perbaikan keamanan aset informasi terkait kendali akses untuk STIE Perbanas dalam penelitian ini akan dikembangkan dari segi manajemen yaitu dengan membuat sebuah prosedur berdasarkan kerangka kerja ISO/IEC:27002:2013. Selama melakukan penelitian ini, peneliti mendapat dukungan dari pihak manajemen STIE Perbanas Surabaya khususnya Bagian TIK dan Bidang Akademik yang merupakan narasumber utama dalam proses penggalian kebutuhan. Narasumber tersebut adalah Pembantu

Ketua Bidang Akademik dan Kasie TIK (Manajemen Jaringan dan Technical Support).

Pada penelitian kali ini penggalian informasi lebih banyak dilakukan terhadap divisi TIK terutama kepada Kasie TIK (Manajemen Jaringan dan Technical support) sebagai narasumber utama dari divisi TIK. Divisi TIK yang ada di STIE Perbanas Surabaya ini memiliki 4 staff dimana 2 orang sebagai programmer, 1 orang sebagai analis, dan 1 orang sebagai kepala TIK. Penelitian ini difokuskan pada divisi TIK karena topik yang diangkat adalah mengenai keamanan aset informasi terkait kendali akses dimana seluruh kendali akses yang terkait dengan sistem informasi di STIE Perbanas langsung diawasi oleh divisi TIK. Beberapa contoh sistem informasi yang dikelola oleh divisi TIK ini adalah SIMAS (Sistem Informasi Akademik dan Kemahasiswaan), SISFO, dan Sistem Informasi Perpustakaan. Selain itu divisi TIK STIE Perbanas juga berwenang dalam pendistribusian hak akses jaringan internet yang ada di Perbanas kepada seluruh mahasiswa, termasuk juga melakukan pembatasan berdasarkan masing-masing kewenangannya. Namun dalam penelitian ini tidak mengesampingkan juga Bapak Emanuel Kristijadi sebagai Pembantu Ketua Bidang Akademik sekaligus sebagai narasumber kedua pada penelitian ini. Ruang lingkup yang akan digali dari narasumber kedua ini adalah terkait dengan bidang manajemennya. Hal-hal yang akan dibahas dengan Pembantu Ketua Bidang Akademik ini adalah mengenai penerapan kebijakan dan SOP yang dibuat nantinya karena Pembantu Ketua Bidang Akademik inilah yang berwenang untuk memberikan izin dan menimbang segala prosedur maupun SOP baru yang akan diterapkan pada suatu divisi tertentu. Sehingga diperlukan verifikasi dan validasi dengan Pembantu Ketua Bidang Akademik agar dokumen yang dibuat sesuai dengan kondisi yang ada di STIE Perbanas Surabaya dan bisa diimplementasikan ke dalam divisi yang dituju.

4.2 Penggalian Data dan Informasi

Pengumpulan data dengan metode interview atau wawancara, yang akan dilaksakan terhadap Bagian TIK dan Bidang Akademik STIE Perbanas selaku perwakilan yang memiliki wewenang dalam teknologi informasi. Berikut ini adalah perancangan proses dari pengumpulan data dan informasi.

Tabel 4. 1 Deskripsi Perancangan Proses Pengumpulan Data dan Informasi

Nama Proses	Pengumpulan Data dan Informasi
Teknik	Wawancara Wawancara adalah sebuah kegiatan penggalian informasi melalui percakapan secara langsung kepada pihak yang berkaitan dengan objek penelitian. Wawancara umumnya menggunakan format tanya jawab yang terencana. Dalam penelitian ini, jenis wawancara yang digunakan adalah wawancara terstruktur, yaitu dengan mempersiapkan pertanyaan.
Objek	Keamanan Aset Informasi terkait Kendali Akses di STIE Perbanas Surabaya
Kebutuhan Proses	*Interview Protocol*
Strategi Pelaksanaan	Untuk mengumpulkan data melalui wawancara perlu dirumuskan strategi pelaksanaan agar pada saat wawancara berlangsung tidak ditemui hambatan. Strategi tersebut dapat berupa urutan tahapan yang akan dilakukan untuk

Nama Proses	Pengumpulan Data dan Informasi
	mempersiapkan wawancara. Tahapan wawancara tersebut adalah sebagai berikut: • Menetapkan tujuan wawancara • Membuat Interview Protocol • Menentukan Narasumber

1. Tujuan Wawancara

Tujuan Wawancara ditetapkan untuk menjadi acuan dalam perumusan pertanyaan wawancara, sehingga proses penggalian data dapat berjalan sesuai dengan tujuan yang diinginkan dan mendapatkan data dan juga informasi yang dibutuhkan dalam penelitian.

Tabel 4. 2 Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan wawancara
1	Pembantu Ketua 1 Bidang Akademik	Penggalian informasi mengenai proses bisnis dalam STIE Perbanas dan fungsi-fungsi yang ada didalamnya, gambaran umum penggunaan teknologi informasi, kebutuhan keamanan data, pengelolaan aset sistem informasi, risiko keamanan yang pernah terjadi dan sering terjadi
2	Bagian TIK	Penggalian informasi mengenai implementasi

Wawancara Ke-	Narasumber	Tujuan wawancara
		teknologi informasi dalam STIE Perbanas termasuk didalamnya yang terkait dengan hal teknis, penggunaan software, database dan jaringan, kelemahan teknologi informasi daris sudut pandang TIK, risiko keamanan yang pernah terjadi dan sering terjadi.

2. Membuat *Interview Protocol*

Interview Protocol adalah daftar pertanyaan yang akan diajukan pada saat wawancara dengan narasumber. Dalam penelitian ini, *interview protocol* akan dibuat dengan berdasarkan pada tujuan wawancara yang sudah ditentukan. Berikut merupakan *interview protocol* dan detail ringkas pertanyaan yang akan diajukan pada saat wawancara.

Tabel 4. 3 Detail Ringkas Pertanyaan dalam Interview Protocol

No	Tujuan Pertanyaan	Detail Ringkas Pertanyaan
1	Penggalian informasi mengenai proses bisnis dalam STIE Perbanas Surabaya dan fungsi-fungsi yang ada di dalamnya, gambaran umum penggunaan	• Aktivitas utama dalam proses bisnis akademik di STIE Perbanas Surabaya • Data struktur organisasi dan peran fungsi yang terlibat dalam proses bisnis • Aset vital dalam operasional • Hak akses terhadap aset vital • Praktek pengamanan yang

No	Tujuan Pertanyaan	Detail Ringkas Pertanyaan
	teknologi informasi, kebutuhan kendali akses, pengelolaan aset informasi, risiko keamanan yang pernah terjadi dan sering terjadi.	telah dilakukan • Identifikasi risiko keamanan aset informasi terkait kendali akses • Seberapa sering risiko terjadi beserta penyebab dan dampaknya
2	Penggalian informasi mengenai implementasi teknologi informasi dalam STIE Perbanas Surabaya termasuk mengenai hal teknis penggunaan software, database dan jaringan, kelemahan teknologi informasi dari sudut pandang TIK, risiko keamanan yang pernah terjadi dan sering terjadi.	• Aktivitas utama bagian TIK • Proses bisnis penerapan TI di STIE Perbanas Surabaya • Aset kritis dalam operasional • Hak ases terhadap akses kritis tersebut • Praktek pengamanan yang telah dilakukan • Identifikasi risiko keamanan aset informasi terkait kendali akses • Seberapa sering risiko terjadi beserta penyebab dan dampaknya.

3. Menentukan Narasumber

Penentuan narasumber dilakukan untuk memudahkan proses pengumpulan data dan informasi. Dalam penetapan pihak narasumber, yang harus diperhatikan adalah kapasitas objek

dalam kewenangannya memberi informasi yang valid, dan apakah pertanyaan yang dirumuskan relevan dengan pengetahuan pihak narasumber. Berikut ini adalah profil narasumber dalam penelitian.

Tabel 4. 4 Narasumber

Nama	Jabatan
Dr. Drs. Emanuel Kritijadi, MM	Pembantu Ketua Bidang Akademik
Hariadi Yutanto, S.Kom, M.Kom	Kasie TIK (Manajemen Jaringan dan Technical Support)

4.3 Perancangan Penilaian Risiko

Dalam melakukan penilaian risiko, peneliti menggunakan pendekatan *risk assessment* kerangka kerja ISO/IEC:27002:2013 dengan metode FMEA (*Failure Modes and Effects Analysis*). Dimana dalam pendekatan *risk assessment* tersebut terdapat beberapa proses dalam melakukan penilaian risiko yaitu menetapkan dan mengelola kriteria, mengidentifikasi risiko, menganalisa risiko dan mengevaluasi risiko.

4.3.1 Kriteria Penilaian Risiko

Dalam melakukan penilaian risiko, metode yang digunakan dalam penelitian adalah dengan metode FMEA. Dalam metode FMEA terdapat kriteria dalam melakukan penilaian risiko yaitu berdasarkan pada nilai dampak (*severity*), nilai kemungkinan (*occurrence*), dan nilai deteksi (*detection*). Berikut adalah kriteria perhitungan untuk masing-masing nilai.

a. Penentuan Nilai Dampak (*Severity* = S)

Pengukuran nilai dampak akan dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi

aspek-aspek penting dalam organisasi. Dalam menentukan penilaian tingkat dampak, perlu dibuat parameter untuk setiap nilainya. Berikut merupakan penjelasan dari masing-masing nilai dampak.

Tabel 4. 5 Kriteria Nilai Dampak

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai Pelanggan atau Karyawan	10
Akibat Serius	Aktivitas yang illegal	9
Akibat Ekstrim	Mengubah Produk atau Jasa menjadi tidak layak digunakan	8
Akibat Major	Menyebabkan ketidakpuasan pelanggan secara ekstrim	7
Akibat Signifikan	Menghasilkan kerusakan parsial secara moderat	6
Akibat Moderat	Menyebabkan penurunan kinerja dan mengakibatkan keluhan	5
Akibat Minor	Menyebabkan sedikit kerugian	4
Akibat Ringan	Menyebabkan gangguan kecil yang dapat diatas tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari: terjadi gangguan kecil pada kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

b. Penentuan Nilai Kemungkinan (*Occurrence* = O)

Pengukuran nilai kemungkinan adalah kemungkinan bahwa penyebab kegagalan akan terjadi dan menghasilkan bentuk kegagalan proses. Nilai kemungkinan merupakan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah

atau gangguan yang dapat menghasilkan kegagalan. Berikut merupakan penjelasan dari nilai kemungkinan.

Tabel 4. 6 Kriteria Nilai Kemungkinan

Kemungkinan Kegagalan	Probablitas	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7
Moderatly High : Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

c. Penentuan Nilai Deteksi (*Detection* = D)

Pengukuran nilai deteksi merupakan penilaian terhadap kemampuan organisasi dalam melakukan kontrol dan kendali terhadap terjadinya suatu gangguan atau kegagalan yang akan terjadi. Berikut adalah penjelasan nilai deteksi dan metode deteksi terhadap risiko.

Tabel 4. 7 Kriteria Nilai Deteksi

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode detensi	10
Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Sangat Rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Rendah	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Sedang	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Cukup Tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan	3
Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2

Deteksi	Kriteria Deteksi	Ranking
Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	1

Setelah melakukan penentuan nilai dampak (*severity)*, nilai kemungkinan (*occurrence*) dan nilai deteksi (*detection*) selanjutnya adalah melakukan kalkulasi nilai prioritas risiko (Risk Priority Number) yang didapatkan dari formulasi berikut:

$$RPN = S \times O \times D$$

RPN : *Risk Priority Number,* perhitungan nilai risiko
S : *Severity,* nilai dampak
O : *Occurrence,* nilai kemungkinan
D : *Detection,* nilai deteksi

4.3.2 Kriteria Penerimaan Risiko

Penentuan kriteria penerimaan risiko didasarkan pada hasil penilaian risiko, dimana setelah ditentukan nilai RPN dari masing-masing risiko, selanjutnya ditentukan level risiko berdasarkan skala RPN. Risiko dengan tingkat *very high* dan *high* kemudian akan dilakukan analisis lebih lanjut untuk menentukan perlakukan risiko. Berikut ini adalah skala penentuan nilai RPN berdasarkan pada metode FMEA.

Tabel 4. 8 Penerimaan Resiko

Level Risiko	Skala Nilai RPN
Very High	>= 200
High	>=120 - < 200

Medium	>=80 - < 120
Low	>=20 - < 80
Very Low	0 - < 20

4.4 Perencanaan Perlakuan Risiko

Dalam perencanaan perlakukan risiko yang dilakukan terlebih dahulu adalah penentuan tujuan control berdasarkan kerangka kerja ISO/IEC:27002:2013. Penentuan tujuan control tersebut dilakukan dengan cara memetakan risiko dengan kategori kendali akses berdasarkan control pada kerangka kerja ISO/IEC:27002:2013.

4.4.1 Pemetaan Risiko dan Kontrol ISO/IEC:27002:2013

Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan control ISO/IEC:27002:2013 yang dibutuhkan dalam melakukan mitigasi terhadap risiko. Berikut adalah tabel pemetaan risiko dengan kategori kendali akses dan control ISO/IEC:27002:2013

Tabel 4. 9 Contoh pemetaan risiko dengan kontrol ISO/IEC : 27002:2013

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO/IEC:27002:2013	Justifikasi
Sumber Daya Mahasiswa	Mahasiswa	26	Manipulasi data	Sharing password mahasiswa/i	*9.1.1 Access Control Policy*	Kontrol yang memuat aturan/kebijakan dalam menggunakan hak akses di sebuah organisasi.

Setelah pemetaan kontrol dengan kerangka kerja ISO/IEC:27002:2013 selesai dilakukan, kemudian dibuatlah daftar rekomendasi mitigasi risiko. Hasil rekomendasi mitigasi

risiko inilah yang akan menjadi bahan pertimbangan untuk usulan perancangan prosedur dan juga kebijakan.

4.4.2 Rekomendasi Mitigasi Risiko

Setelah melakukan pemetaan risiko berdasarkan kontrol ISO/IEC:27002:2013, maka hal yang berikutnya dilakukan adalah menentukan mitigasi risiko. Mitigasi risiko ini didasarkan pada standard ISO/IECL:27002:2013. Luaran yang dihasilkan dari penentuan mitigasi risiko ini adalah prosedur atau kebijakan yang diperlukan untuk memastikan risiko tidak terulang kembali. Berikut ini adalah tabel rekomendasi mitigasi risiko.

Tabel 4. 10 Contoh Rekomendasi Mitigasi Risiko

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Rekomendasi Mitigasi Risiko	Prosedur yang dihasilkan
Sumber Daya Mahasiswa	Mahasiswa	26	Manipulasi data	Sharing password mahasiswa/i	Membuat ***kebijakan kendali akses***	Kebijakan kendali akses

4.5 Perencanaan Pengujian SOP

Pengujian SOP ini dilakukan melalui dua cara yakni verifikasi dan validasi. Verifikasi dilakukan dengan cara wawancara untuk memastikan kebenaran informasi yang terkandung dalam SOP, sedangkan validasi dilakukan dengan simulasi untuk mengetahui ketepatan SOP ketika implementasi dalam kasus nyata.

Tabel 4. 11 Metode Pengujian SOP

Tujuan		Metode	Sasaran
Verifikasi	Untuk melakukan verifikasi terhadap dokumen guna memastikan kebenaran dari informasi-informasi yang didefinisikan dan termuat di dalam dokumen SOP	Wawancara	*Key User* (pihak yang memiliki kedudukan penting dalam bagian TIK STIE Perbanas Surabaya dan memiliki kewenangan untuk mendefiinisikan kebutuhan keamanan) yaitu *Kasie TIK STIE Perbanas Surabaya*
Validasi	Untuk melakukan validasi dokumen dengan melihat apakah SOP dapat berjalan sesuai dengan kondisi yang ada dan untuk menemukan kekurangan dari SOP yang telah dibuat sehingga dapat dilakukan koreksi dan selanjutnya dapat diterapkan	Simulasi Pengujian Dokumen SOP	Pelaksana SOP, yakni : Pegawai Bagian TIK (administrator aplikasi dan jaringan)

4.5.1 Verifikasi

Verifikasi dilakukan dengan tujuan memastikan kebenaran dari informasi yang termuat dalam dokumen SOP dan kesesuaiannya dengan kondisi STIE Perbanas Surabaya. Metode yang digunakan dalam melakukan verifikasi adalah dengan wawancara kepada bagian TIK STIE Perbanas sebagai pihak yang memiliki kewenangan dalam keamanan teknologi informasi. Berikut adalah tahapa yang dilakukan dalam melakukan verifikasi pengujian SOP:

1. Penulis meneyerahkan dokumen SOP kepada bagian TIK dan menjelaskan isi dokumen secara detail.
2. Bagian TIK melakukan review dokumen SOP
3. Penulis mengadakan wawancara secara langsung setelah Bagian TIK selesai mereview dokumen. Pertanyaan yang dilontarkan terkait struktur SOP, konten SOP, serta istilah yang digunakan dalam SOP.
4. Bagian TIK memberikan review dan revisi dokumen jika ada
5. Penulis melakukan pembenahan dokumen SOP sesuai saran dari Bagian TIK.
6. Penulis menyerahkan ulang hasil revisi pada bagian TIK.
7. Bagian TIK menyetujui dokumen SOP yang telah diperbaiki.

4.5.2 Validasi

Validasi dilakukan untuk memastikan dokumen SOP dapat berjalan sesuai dengan kondisi yang ada pada STIE Perbanas dan untuk menemukan ketidaksesuaian dan kekurangan SOP sehingga dapat dibenahi sesuai dengan kondisi yang ada. Metode yang digunakan adalah dengan pengujian SOP dengan pelaksanan SOP nya adalah bagian TIK. Berikut merupakan tahapan yang dilakukan dalam melakukan validasi pengujian SOP:

1. Penulis menyerahkan dokumen SOP yang telah diperbaiki pada tahap verifikasi.

2. Penulis memberikan arahan penggunaan dokumen SOP dan menjelaskan beberapa skenario yang akan diuji.
3. Pelaksanan SOP mensimulasikan SOP dengan menggunakan case yang masuk pada service desk, termasuk mengisi form-form yang tersedia.
4. Setelah simulasi selesai, penulis meminta *feedback* dan *review* dari pelakasana.
5. Penulis melakukan perbaikan dokumen jika terdapat ketidaksesuaian pada proses simulasi.
6. Setelah selesai, dokumen SOP dapat dinyatakan valid dan dapat diterapkan.

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang implementasi setiap tahapan dan proses-proses di dalam metodologi tugas akhir yang dapat berupa hasil, waktu pelaksanaan dan lampiran terkait yang memuat pencatatan tertentu dengan implementasi proses.

5.1 Penggalian Kondisi Existing

Penggalian kondisi existing yang dilakukan dalam penelitian bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan keamanan aset informasi terkait kendali akses pada STIE Perbanas Surabaya. Dalam melakukan penggalian kondisi existing, dilakukan wawancara menggunakan *interview protocol* dengan Pembantu Ketua Bidang Akademik dan Kepala SIE TIK STIE Perbanas. Berikut adalah hasil identifikasi risiko yang dapat ditarik dari hasil wawancara mengenai risiko keamanan aset informasi terkait kendali akses.

5.1.1 Identifikasi Aset Kritis

Penentuan aset kritis dilakukan melalui pengumpulan informasi berdasarkan sudut pandang pihak manajemen STIE Perbanas yaitu Pembantu Ketua 1 Bidang Akademik dan Ketua SIE TIK. Justifikasi penentuan aset kritis ini juga dilakukan dengan cara melakukan observasi secara langsung dan diskusi dengan pihak yang terkait. Dari observasi dan pengamatan langsung yang dilakukan oleh peneliti, kemudian hasil tersebut dipaparkan kepada narasumber untuk kemudian divalidasi, apakah hasil yang didapat sudah sesuai dengan kondisi yang ada di Perbanas atau belum. Selain itu dilakukan juga wawancara dengan hasil yang terlampir pada Lampiran A dan Lampiran B maka dapat disimpulkan bahwa dalam masing-masing kategori Aset TI terdapat aset kritis yang dijelaskan dalam tabel berikut ini.

Tabel 5. 1 Daftar Aset Kritis

Kategori Aset	Aset Kritis	Alasan/Sebab
Hardware	Server PC	Server dan PC menjadi pendukung dalam proses bisnis akademik. Server menjadi aset penting untuk memastikan data dan informasi selalu dapat diakses dan komputer digunakan untuk proses operasional Bagian TIK dan juga sebagai media untuk mengakses data.
Software	SISFO E-Learning (kuliah.perbanas.ac.id) Sistem Informasi Perpustakaan	Aplikasi SISFO, E-Learning, dan perpustakaan merupakan pendukung kegiatan akademik. Dalam SISFO yang informasinya saling terintegrasi, salah satu modul yang paling penting adalah SIMAS sebagai sistem informasi akademik mahasiswa yang berisikan data akademik dan demografi mahasiswa. Dalam E-Learning Data dan informasi penting yang terkait adalah mengenai materi ajar dosen. Sedangkan dalam Sistem Informasi Perpustakaan data dan informasi penting yang terkait adalah mengenai keseluruhan penelitian yang dilakukan pada STIE Perbanas.
Data	Data Demografi Mahasiswa Data	Data terkait akademik, demografi mahasiswa penting dalam proses kegiatan akademik dan data file server

Kategori Aset	Aset Kritis	Alasan/Sebab
	Akademik Data File Server	penting dalam kegiatan/proses perkuliahan pada STIE Perbanas. Seluruh data hampir dibutuhkan oleh semua komponen.
Jaringan	Wifi Kabel Router	Jaringan digunakan untuk mengakses informasi, seperti mengakses database dan mengakses internet.
Sumber Daya Manusia	Dosen Mahasiswa Pegawai	Suatu aset yang penting dalam sebuah organisasi karena SDM yang memiliki kompetensi dapat mendukung proses bisnis berjalan dengan lancer.

5.1.2 Identifikasi Kebutuhan Keamanan Aset Kritis

Kebutuhan keaman merupakan bentuk perlindungan terhadap ancaman yang mungkin terjadi dalam upaya untuk memastikan keberlangsungan proses bisnis, meminimalisir risiko bisnis. Kebutuhan keamanan tiap-tiap aset juga memiliki lebih dari satu kebutuhan. Justifikasi kebutuhan keamanan aset kritis ini juga dilakukan dengan cara melakukan observasi secara langsung dan diskusi dengan pihak yang terkait. Dari observasi dan pengamatan langsung yang dilakukan oleh peneliti, kemudian hasil tersebut dipaparkan kepada narasumber untuk kemudian divalidasi, apakah hasil yang didapat sudah sesuai dengan kondisi yang ada di Perbanas atau belum. Berikut ini adalah daftar kebutuhan keamanan aset kritis pada STIE Perbanas.

Tabel 5. 2 Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Keamanan	Narasumber
Server	Dapat diakses 24 jam dalam 7 hari	Bagian TIK
	Konfigurasi server dilakukan dengan benar	Bagian TIK
	Adanya sumber listrik cadangan	Bagian TIK
	Adanya kontrol keamanan untuk ruang fisik server	Bagian TIK
	Adanya pembatasan hak akses	Bagian TIK
	Server tidak boleh diakses oleh usb atau pihak yang tidak berwenang yang dapat mengubah konten	Bagian TIK
PC	Dapat berfungsi selama jam kerja organisasi	Bagian TIK
	Adanya sumber listrik cadangan	Bagian TIK
	Adanya antivirus	Bagian TIK
	Adanya pembatasan hak akses	Bagian TIK
	Data-data yang terdapat di dalam pc harus lengkap dan harus memiliki login agar terjaga kerahasiaannya	Bagian TIK

Aset Kritis	Kebutuhan Keamanan	Narasumber
SISFO (Sistem Informasi)	Dapat diakses 24 jam dalam 7 hari	Bagian TIK
E-learning	Data dapat diakses 24 jam dalam 7 hari	Bagian TIK
Perpustakaan	Adanya backup data secara rutin	Bagian TIK
	Data-data yang terkait dalam aplikasi harus lengkap dan akurat	Bagian Akademik
Data Demografi Mahasiswa	Adanya pembatasan hak akses	Bagian TIK
	Adanya pengamanan terhadap informasi yang ada di dalamnya	Bidang akademik
Data Akademik	Adanya pengamanan terhadap informasi yang ada di dalamnya	Bidang akademik
Data File Server	Adanya pembatasan hak akses pegawai pada data tertentu	Bagian TIK
	Data-data harus lengkap dan akurat	Bidang akademik
Wifi	Tersedia selama jam operasional kerja organisasi	Bagian TIK
	Terdapat sumber listrik cadangan	Bagian TIK

Aset Kritis	Kebutuhan Keamanan	Narasumber
	Adanya kontrol rutin	Bagian TIK
	Adanya anti netcut	Bagian TIK
Kabel	Tersedia selama jam operasional kerja organisasi	Bagian TIK
	Adanya kontrol rutin	Bagian TIK
	Kabel dilakukan pelabelan untuk mempermudah pengorganisasian	Bagian TIK
Router	Tersedia selama jam operasional kerja organisasi	Bagian TIK
	Adanya kontrol rutin	Bagian TIK
	Memonitoring jaringan untuk memastikan keaslian data maupun informasi	Bagian TIK

5.1.3 Identifikasi Ancaman Aset Kritis

Ancaman aset kritis merupakan hal yang mungkin terjadi dan pernah terjadi pada aset dan mengakibatkan terganggunya proses bisnis. Identifikasi ancaman pada aset kritis dikategorikan sesuai dengan daftar aset kritis yang ada. Daftar ancaman berikut ini didapatkan dari hasil wawancara kepada narasumber. Selain itu justifikasi ancaman aset kritis ini juga dilakukan dengan cara melakukan observasi secara langsung dan diskusi dengan pihak yang terkait. Dari observasi dan pengamatan langsung yang dilakukan oleh peneliti, kemudian hasil tersebut dipaparkan kepada narasumber untuk kemudian divalidasi, apakah hasil yang didapat sudah sesuai dengan

kondisi yang ada di Perbanas atau belum. Berikut adalah daftar ancaman aset kritis pada STIE Perbanas Surabaya.

Tabel 5. 3 Identifikasi ancaman aset kritis

Aset Kritis	Kemungkinan Ancaman
Server	• Bencana alam (gempa bumi, badai dan petir, banjir, kebakaran) • Genset tidak dapat berfungsi karena mengalami kerusakan • Listrik mati • Terserang virus • Adanya pencurian data maupun informasi oleh hacker
PC	• Bencana alam (gempa bumi, badai dan petir, banjir, kebakaran) • Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Pencurian data maupun informasi • Pencurian hardware
SISFO (Sistem Informasi)	• Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Terjadinya manipulasi data yang dilakukan oleh hacker
E-learning	• Listrik mati • Genset tidak dapat berfungsi karena

Aset Kritis	Kemungkinan Ancaman
	mengalami kerusakan • Terserang virus • Terjadinya manipulasi data yang dilakukan oleh hacker
Perpustakaan	• Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Terjadinya manipulasi data yang dilakukan oleh hacker
Data demografi mahasiswa	• Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Terjadinya manipulasi data yang dilakukan oleh hacker • Terjadinya pencurian data yang dilakukan oleh hacker
Data akademik	• Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Terjadinya manipulasi data yang dilakukan oleh hacker • Terjadinya pencurian data yang dilakukan oleh hacker
Data file server	• Listrik mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Terserang virus • Terjadinya manipulasi data

Aset Kritis	Kemungkinan Ancaman
	yang dilakukan oleh hacker • Terjadinya pencurian data yang dilakukan oleh hacker
Wifi	• Listrik mati • Internet mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Adanya netcut yang dilakukan oleh oknum yang tidak bertanggung jawab • Adanya gangguan terhadap koneksi internet • Pencurian bandwith oleh hacker
Kabel	• Kerusakan kabel yang diakibatkan oleh hewan maupun manusia
Router	• Listrik mati • Internet mati • Genset tidak dapat berfungsi karena mengalami kerusakan • Adanya netcut yang dilakukan oleh oknum yang tidak bertanggun jawab • Adanya gangguan terhadap koneksi internet • Pencurian perangkat router • Pencurian bandwith oleh hacker

5.1.4 Identifikasi Praktik Keamanan yang telah dilakukan Organisasi

Berikut ini merupakan daftar praktik keamanan yang telah dilakukan STIE Perbanas dalam memastikan keamanan teknologi informasi dapat mendukung berjalannya proses bisnis.

Tabel 5. 4 Daftar Praktik Keamanan yang telah dilakukan Organisasi

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Adanya antivirus (e-scan) dan diupdate terus menerus	Bagian TIK
Adanya update patch dan firewall secara berkala	Bagian TIK
Telah dipasang anti netcut untuk keamanan Wifi	Bagian TIK
Pada Lab tidak bisa memasang USB	Bagian TIK
Pada Lab tidak bisa menginstall aplikasi dari luar	Bagian TIK
Telah dipasang Smoke Detector pada ruang server untuk memberi peringatan apabila terjadi kebakaran	Bidang Umum
Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran	Bidang Umum
Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	Bagian TIK
Telah dilakukan backup server dan NAS setiap hari pukul 19.00	Bagian TIK
Ada penguncian/penggembokan pada ruang server sehingga tidak dapat sembarang orang bisa masuk	Bagian TIK
Data hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja	Bagian TIK
Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk kelas dan lab	Bagian TIK
Dilakukan maintenance setiap sebelum UTS dan UAS hanya untuk lab saja	Bagian TIK
Dilakukan maintenance Wifi setiap 2 minggu sekali	Bagian TIK
Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan	Bagian TIK

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
fungsinya	
Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel	Bagian TIK
Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI di organisasi	Bagian TIK
Adanya log setiap aktivitas dalam sistem informasi SISFO	Bagian TIK

5.1.5 Identifikasi Kerentanan pada Teknologi

Berikut merupakan daftar kerentanan pada teknologi yang dibagi kedalam masing-masing aset kritis.

Tabel 5. 5 Daftar Kerentanan pada Teknologi

Server	
System of Interest	Server yang menyimpan Data Penting
Komponen Utama	**Kemungkinan Kerentanan**
• Sistem Operasi • Processor • RAM • Harddisk • Listrik • Keamanan Jaringan • Genset • UPS • Kabel • Smoke Detector • Ruang Server	• RAM mengalami *overload* • Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (Harddisk) penuh • UPS tidak berfungsi • Tidak terdapatnya pengamanan yang kuat pada ruang server • Lemahnya sistem pengamanan jaringan • Kerusakan pada server
PC	
System of Interest	PC yang ada pada kampus I dan II

	STIE Perbanas
Komponen Utama	**Kemungkinan Kerentanan**
• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall	• Monitor, Keyboard ataupun mouse mengalami kerusakan karena pemakian berlebih • Sistem pengamanan firewall yang lemah • UPS tidak berfungsi • Antivirus yang masih kurang kuat untuk mencegah virus • Terdapatnya bug pada software • Performa sistem yang kurang maksmial karena sistem operasi tidak asli • Kesalahan konfigurasi hardware • Terjadi pencurian pada perangkat PC
Data	
System of Interest	Data Demografi Mahasiswa, Data Akademik dan Data File Server
Komponen Utama	**Kemungkinan Kerentanan**
• Database • Server • Listrik • PC • Firewall • Database Administrator (DBA)	• Sistem pengamanan firewall yang lemah • Kerusakan pada PC • Database Admnistrator salah dalam melakukan pengolahan data (ubah dan hapus) • Kurangnya kontrol keamanan database yang dilakukan oleh Database Administrator
Perangkat Lunak	
System of Interest	SIMAS, E-learning dan Perpustakaan
Komponen Utama	**Kemungkinan Kerentanan**
• Firewall • Server • Antivirus	• Sistem pengamanan firewall yang lemah • Antivirus yang masih kurang kuat

	untuk mencegah virus • Server mengalami kerusakan sehingga sistem tidak dapat diakses • Bug pada software • Kesalahan konfigurasi pada sistem
Wifi	
System of Interest	18 Wifi yang terpasang pada kampus I STIE Perbanas dan 3 Wifi yang terpasang pada kampus II STIE Perbanas
Komponen Utama	**Kemungkinan Kerentanan**
• Listrik • Kabel • Keamanan Jaringan	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Terjadinya konsleting pada kabel • Sistem keamanan jaringan yang lemah
Router	
System of Interest	Router
Komponen Utama	**Kemungkinan Kerentanan**
• Listrik • Kabel • Keamanan Jaringan	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Terjadinya konsleting pada kabel • Sistem keamanan jaringan yang lemah • Kesalahan konfigurasi pada router

5.1.6 Hubungan antara Aset Kritis, Kebutuhan Keamanan, Ancaman dan Praktik Keamanan Organisasi

Berdasarkan hasil analisis terkait aset kritis, kebutuhan keamanan, ancaman untuk masing-masing aset dan juga praktik keamanan yang telah dilakukan oleh STIE Perbanas, maka perlu dilakukan pemetaan hubungan antara masing-masing aset dengan identifikasi kebutuhan keamanan dan

ancaman serta praktik keamanan yang telah dilakukan. Pemetaan hubungan tersebut berfungsi untuk menganalisis lebih dalam kondisi kekinian dari praktik keamanan yang telah dilakukan oleh STIE Perbanas untuk mengatasi adanya ancaman untuk setiap aset kritis. Beriktu ini adalah hubungan antara aset kritis dan masing-masing kebutuhan keamanan, ancaman serta praktik keamanan yang telah diimplementasikan.

Tabel 5. 6 Hubungan antara aset kritis, kebutuhan keamanan, ancaman, dan praktik keamanan organisasi

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
Hardware	Server	Dapat diakses 24 jam dalam 7 hari	• Kerusakan Komputer • Kerusakan Server • Kerusakan Genset dan UPS • Kesalahan konfigurasi • Pencurian hardware	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk perangkat TI pada setiap kelas dan lab • Dilakukan maintenance setiap sebelum UTS dan UAS hanya untuk perangkat TI pada Lab saja • Pada ruang server telah dipasang smoke detector untuk memberikan peringatan apabila terhadi kebakaran • Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran • Ada penguncian pada ruang
		Konfigurasi server dilakukan dengan benar		
		Adanya sumber listrik cadangan		
		Adanya kontrol keamanan untuk ruang fisik server		
		Adanya pembatasan hak akses		
		Server tidak boleh diakses oleh usb atau pihak yang tidak berwenang yang dapat mengubah konten		
	PC	Dapat berfungsi selama jam kerja organisasi		
		Adanya sumber listrik		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
		cadanagn		server dan kunci selalu dipegang oleh Bagian TIK • Pembuatan dan pelaksanaan beberapa SOP tekait pengelolaan perangkat TI oleh Bagian TIK
		Adanya Antivirus		
		Adanya pembatasan hak akses		
		Data-data yang terdapat didalam pc harus lengkap dan harus lengkap dan harus memiliki login agar kerahasiaan terjaga		
Software	SISFO (Sistem Informasi)	Dapat diakses 24 jam dalam 7 hari	• Bug pada software • Virus/worm • Kesalahan konfigurasi sistem • Pembobolan sistem	• Adanya antivirus (e-scan) dan telah di update terus menerus setiap hari • Pada lab tidak dapat dipasang USB • Pada lab tidak dapat di install aplikasi dari luar • Telah dilakukan sosialisasi keapda mahasiswa dan dosen untuk praktik keamanan TI
	E-Learning	Data dapat diakses 24 jam dalam 7 hari		
	Sistem Informasi Perpustakaan	Adanya backup data secara rutin		
		Data-data terkait dalam		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
		aplikasi harus lengkap dan akurat		• Membedakan role dan hak akses untuk masing masing pegawai sesuai dengan unit kerja
Data	Data Demografi Mahasiswa	Adanya pembatasan hak akses	• Kesalahan input data • Data corrupt/rusak • Pencurian data • Sharing password	• Telah dilakukan back up server dan NAS setiap hari secara berkala dan terjadwal • Data hanya dapat dimasukkan, diganti dan dihapus oleh database administrator saja • Adanya perbedaan role atau hak akses pada data untuk masing masing fungsi
		Adanya pengamanan terhadap data		
	Data Akaemik	Adanya pengamanan terhadap data		
	Data file server	Adanya pembatasan hak akses pegawai pada data		
		Data-data harus lengkap dan akurat		
Jaringan	Wifi	Tersedia selama jam operasional kerja organisasi	• Gangguan pada router • Kerusakan kabel • Gangguan koneksi internet	• Telah dipasang anti netcut untuk keamanan wifi • Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk setiap
		Terdapat sumber listrik cadangan		
		Adanya kontrol rutin		
		Adanya anti netcut		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
	Kabel	Tersedia selama jam operasional kerja organisasi	• Sabotase jaringan internet	perangkat TI • Dilakukan maintenance WIFI setiap 2 minggu sekali • Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabell • Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI oleh Bagian TIK
		Adanya kontrol rutin		
		Kabel dilakukan pelabelan untuk mempermudah pengorganisasian		
	Router	Tersedia selama jam operasional kerja organisasi		
		Adanya kontrol rutin		
		Memonitoring jaringan untuk memastikan keaslian data		

5.2 Analisis Risiko

Analisis risiko didasarkan pada hasil identifikasi kebutuhan keamanan, ancaman dan juga praktik keamanan dari masing-masing aset kritis yang telah diidentifikasi sebelumnya. Analisis risiko dilakukan dengan berdasarkan pada metode FMEA. Dimana sebelum melakukan analisis risiko terdapat dua proses utama yang akan dilakukan yaitu identifikasi risiko dan penilaian risiko. Dalam melakukan analisis risiko, terlebih dahulu dilakukan identifikasi potensi penyebab kegagalan dan potensi dampak kegagalan untuk setiap risiko. Setelah daftar risiko beserta penyebab dan dampak diidentifikasi, selanjutnya adalah melakukan penilaian risiko berdasarkan kriteria penilaian risiko pada metode FMEA. Penilaian risiko yang dilakukan secara menyeluruh dan didasarkan pada seluruh komponen sistem informasi yaitu *hardware, software,* jaringan, data dan sumber daya manusia. Sehingga dalam tahap analisis risiko akan dihasilkan luaran sebuah *risk register* beserta hasil penilaian risiko.

5.2.1 Risk Register

Berikut ini merupakan *risk register* untuk risiko keamanan aset informasi terkait kendali akses yang didasarkan pada risiko yang mungkin timbul pada kelima aset kritis yang bias menghambat atau bahkan merugikan proses bisnis yang ada di STIE Perbanas Surabaya. Dan untuk keseluruhan daftar risiko dapat dilihat pada Lampiran C.

Tabel 5. 7 Risk Register untuk Keamanan Aset Informasi terkait Kendali Akses

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
Sumber Daya Manusia	Mahasiswa	26	Manipulasi data	Sharing password mahasiswa/i	Komplain dari civitas akademika	Mahasiswa
Data	Data demografi mahasiswa, data akademik dan data file server	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	Komplain dari civitas akademika dan berkurangnya kepercayaan civitas akademika	*Pengguna SISFO*
		13	Manipulasi data	Terdapat hacker yang memanipulasi	Komplain dari civitas akademika	*Bagian TIK*

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
				data	dan berkurangnya kepercayaan civitas akademika	
		12	Pencurian data	Terdapat hacker yang mencuri data	Berkurangnya kepercayaan civitas akademika	*Bagian TIK*
Software	SIMAS (Sistem Informasi Mahasiswa), E-learning, Perpustakaan	10	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	Tersebar luasnya data organisasi	*Organisasi*

5.2.2 Penilaian Risiko dengan Metode FMEA

Penilaian ini sesuai dengan kriteria penilaian risiko berdasarkan metode FMEA. Berikut ini merupakan hasil penilaian untuk risiko keamanan aset informasi terkait kendali akses dengan tingkat *very high* hingga *low.* Sedangkan untuk keseluruhan penilaian risiko dapat dilihat pada Lampiran C.

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Sharing Password Mahasiswa/i	Komplain dari civitas akademika Penurunan citra organisasi	7	Penyebaran password oleh mahasiswa memiliki dampak yang besar karena data dalam masing masing akun mahasiswa bersifat rahasia, dan sistem *change password* belum dimiliki dalam sistem kemahasiswaannya dan hanya admin yang dapat mengubah passoword	Manipulasi data	6	Terjadi hampir disetiap FRS semester baru walau dengan kasus yang tidak banyak	Sosialisasi kepada mahasiswa/i	5	Kontrol yang dilakukan kurang dapat mengatasi kurangnya awareness mengenai pentingnya menjaga kerahasiaan data	210	Very High	Penggguna SISFO

Gambar 5. 1 Penilaian untuk risiko sharing password mahasiswa/i

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				akademik dan hal ini dapat mengakibatkan berkurangnya kepercayaan civitas dan dampak yang diakibatkan cukup tinggi			telah dilakukan						
	Manipulasi data	Komplain dari civitas akademika	8	Manipulasi data akademik dan mahasiswa dapat mengakibatkan komplain dan	Username dan password diketahui oleh pengguna lain	5	Kemungkinan terjadi setiap tahunnya	Diadakan sosialisasi kepada civitas akademika	5	Kontrol yang dilakukan sudah cukup untuk meningkatkan awareness civitas terhadap data *confidential*	200	Very High	Pengguna SISFO

Gambar 5. 2 Penilaian untuk risiko username dan password diketahui oleh pengguna lain

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				berkurangnya kepercayaan civitas terhadap pengamanan yang sudah dilakukan oleh organisasi sehingga hal ini berdampak cukup tinggi karena beberapa data bersifat *confidential*	pengguna lain					terhadap data *confidential*			
		Berkurangnya kepercayaan civitas akademika			Terdapat hacker yang memanipulasi data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Adanya firewall dan sosialisasi dari Bagian TIK ke civitas	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	**160**	High	Bagian TIK

Gambar 5. 3 Penilaian untuk risiko terdapat hacker yang memanipulasi data

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Pencurian data	Berkurangnya kepercayaan civitas akademika	7	Pencurian data dapat mengakibatkan tersebarnya data dan bocornya data penting akademik dan hal ini dapat mengakibatkan berkurangnya kepercayaan civitas dan dampak yang diakibatkan cukup tinggi	Terdapat hacker yang mencuri data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Adanya firewall dan pengamanan jaringan	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	140	High	Bagian TIK

Gambar 5. 4 Penilaian untuk risiko terdapat hacker yang mencuri data

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
Software	Aplikasi diakses oleh pihak yang tidak berwenang	Tersebarluasnya data orgnisasi	8	Dengan diaksesnya aplikasi oleh pihak yang tidak berwenang dapat mengakibatkan bocornya data akademik dan kemahasiswaan serta data lain yang sifatnya *confidential* sehingga dapat yang diakibatkan sangat tinggi	Kesalahan dalam pemberian hak akses	4	Kemungkinann terjadinya kecil	Adanya peraturan dalam pembatasan hak akses	4	Kontrol yang dilakukan sudah cukup baik namun masih kurang mampu faktor eksternal yang berusaha masuk kedalam sistem	**128**	High	Bagian TIK

Gambar 5. 5 Penilaian untuk risiko kesalahan dalam pemberian hak akses

Tabel 5. 8 Hasil Penilaian Risiko

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
Very High	Manipulasi Data	Sharing password mahasiswa/i	210	2
		Username dan password diketahui oleh pengguna lain	200	
High	Manipulasi Data	Terdapat hacker yang memanipulasi data	160	3
	Pencurian Data	Terdapat hacker yang mencuri data	140	
	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	128	
Low	Akses internet lambat	Ada yang melakukan netcut	70	6
	Penyalahgunaan data organisasi	Adanya praktik KKN di perusahaan	30	
	Pelanggaran regulasi hak akses	Penyalahgunaan akses regulasi	27	
	Penyalahgunaan data organisasi	Adanya praktik KKN di perusahaan	45	
	Pelanggaran regulasi	Penyalahgunaan akses regulasi	36	

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN	Jumlah
	Penyalahgunaan data organisasi	Adanya praktik KKN di perusahaan	30	

5.2.3 Daftar Prioritas Risiko

Dalam tahap analisa risiko ini juga akan dibuat sebuah daftar prioritas risiko yang didasarkan pada level risiko yaitu berdasarkan nilai RPN untuk risiko yang berkaitan dengan keamanan aset informasi terkait kendali akses. Level risiko yang akan diprioritaskan merupakan yang berada pada level risiko *very high,* dan *high.* Berikut ini merupakan tabel daftar prioritras risiko dimana terdapat 5 risiko keamanan aset informasi terkait kendali akses dengan tingkat prioritas tertinggi dilihat dari nilai RPN yang tinggi.

Tabel 5. 9 Daftar Prioritas Risiko

Kategori aset informasi kritis	Aset Informasi kritis	ID Risiko	Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan
Sumber Daya Manusia	Mahasiswa	26	Very High	Manipulasi data	Sharing Password Mahasiswa/i
Data	Data demografi mahasiswa, Data Akademik dan Data File Server	13	Very High	Manipulasi data	Username dan password diketahui oleh pengguna lain
		13	High	Manipulasi data	Terdapat hacker yang memanipulasi data
		12	High	Pencurian data	Terdapat hacker yang mencuri data
Software	SIMAS, E-learning, Perpustakaan	10	High	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses

5.3 Penentuan Klausul

Pada tahap ini, penentuan klausul akan didasasrkan pada daftar prioritas risiko yang sudah didapatkan dari hasil analisis risiko sebelumnya. Penentuan klausul ini mengacu pada kerangka kerja ISO/IEC:27002:2013. Pada penelitian kali ini akan difokuskan kepada masalah keamanan aset informasi kendali akses, dimana di dalam ISO/IEC:27002:2013 terdapat pada point 9.Access Control, klausul tersebut bersangkutan langsung terhadap penelitian kali ini dimana kontrol yang ada di dalam klausul tersebut dapat digunakan untuk melakukan mitigasi risiko yang ada. Dalam klausul *Access Control* yang ada di ISO/IEC:27002:2013 terdapat 15 kontrol, namun hanya 6 kontrol yang digunakan dalam penelitian kali ini.

5.4 Justifikasi Kontrol Risiko

Tahap justifikasi kontrol risiko ini merupakan tahap dalam menentukan tindakan mitigasi risiko yang tepat. Tahap justifikasi kontrol risiko ini dilakukan dengan melakukan pemetaan risiko terhadap masing-masing kontrol yang dibutuhkan ke dalam kerangka kerja ISO/IEC:27002:2013 serta menganalisis rekomendasi mitigasi risiko.

Risiko dengan prioritas tertinggi dipetakan ke dalam kontrol kerangka kerja ISO/IEC:27002:2013. Tujuan dari pemetaan risiko ke dalam kontrol kerangka kerja adalah untuk memastikan perlakuan risiko telah tepat dan sesuai dengan *control objective* dari setiap kontrol kerangka kerja. Selain itu proses ini juga memiliki fungsi untuk memastikan bahwa kontrol yang ada sesuai dengan risiko yang akan dimitigasi.

Setelah melakukan pemetaan risiko terhadap ISO/IEC:27002:2013, selanjutnya akan ditentukan rekomendasi mitigasi risiko berdasarkan kontrol yang telah ditentukan. Rekomendasi mitigasi risiko yang telah dipetakan sesuai dengan risiko dan kebutuhan kontrolnya nantinya akan mendefiniskan usulan-usulan perbaikan dalam sistem informasi SIS STIE Perbanas Surabaya dan juga sebagai input

untuk membuat dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi terkait Kendali Akses pada STIE Perbanas Surabaya.

5.4.1 Pemetaan Risiko dengan Kontrol ISO/IEC:27002:2013

Dalam pemetaan kontrol dengan kerangka kerja ISO/IEC:27002:2013 terdapat 6 kontrol yang digunakan yaitu *9.1.1 Access Control Policy, 9.3.1 Use of Secret Authentication Information, 9.2.1 User Registration and De-registration, 9.4.2 Secure Log-on Procedure, 9.1.2 Access to Networks and Networks Services,* dan *9.4.3 Password Management System.* Berikut adalah pemetaan risiko dan kontrol ISO/IEC:27002:2013, untuk justifikasi pemetaan risiko lihat Lampiran D.

Tabel 5. 10 Pemetaan Risiko dan Kebutuhan Kontrol Pada ISO/IEC:27002:2013

Kategori Aset Informasi Kritis	ID Risiko	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO/IEC:27002:2013
Sumber Daya Manusia	26	Manipulasi data	Sharing password mahasiswa/i	*9.1.1 Access control policy*
Data	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	*9.2.1 User registration and de-registration*
				9.4.3 Password management system
			Terdapat hacker yang memanipulasi	*9.1.2 Access to networks and network*

Kategori Aset Informasi Kritis	ID Risiko	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO/IEC:27002:2013
			data	*services*
	12	Pencurian data	Terdapat hacker yang mencuri data	*9.4.2 Secure log-on procedures*
Software	10	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	*9.3.1 Use of Secrets Authentication Information*

5.4.2 Rekomendasi Mitigasi Risiko

Rekomendasi mitigasi risiko yang dihasilkan akan didasarkan pada kontrol objektik dan petunjuk pelaksanaan pada kerangka kerja ISO/IEC:27002:2013. Selain itu, rekomendasi risiko juga didasarkan identifikasi praktik keamanan yang telah diimplementasikan terhadap risiko yang sudah ada, hal ini berfungsi untuk memastikan tidak ada redudansi tindakan mitigasi risiko dalam mengelola risiko yang muncul. Dalam rekomendasi mitigasi risiko akan didefinisikan input untuk membuat dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi terkait kendali akses pada STIE Perbanas Surabaya dan juga usulan-usulan perbaikan dalam sistem informasi SISFO STIE Perbanas Surabaya. Pemetaan rekomendasi mitigasi risiko dari kontrol kerangka kerja ISO/IEC:27002:2013 dapat dilihat pada lampiran E.

5.5 Prosedur yang Dihasilkan Berdasarkan Hasil Rekomendasi Mitigasi Risiko

Berdasarkan hasil rekomendasi mitigasi risiko yang ada pada Lampiran E, maka dapat dianalisa bahwa untuk mengelola risiko keamanan aset informasi terkait kendali akses yang memiliki prioritas tertingga pada STIE Perbanas diperlukan beberapa prosedur. Prosedur tersebut berfungsi untuk memastikan bahwa risiko yang ada tidak berulang dengan menstandarisasikan proses dan meminimalkan variasi pelaksanaan suatu kegiatan operasional. Berikut ini adalah prosedur yang dihasilkan berdasarkan pada hasil rekomendasi mitigasi risiko pada Lampiran E.

(halaman ini sengaja dikosongkan)

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

6.1 Dokumen Prosedur Mutu Bagian TIK STIE Perbanas Surabaya

Bagian TIK STIE Perbanas telah memiliki beberapa prosedur yang terdokumentasi yang terdiri dari dokumen mengenai standard prosedur suatu aktivitas yang dilakukan oleh bagian TIK yang disebut dengan prosedur mutu dan juga beberapa instruksi kerja. Berikut merupakan penjelasan singkat mengenai masing-masing prosedur mutu dan instruksi kerja yang telah diimplementasikan.

Tabel 6. 1 Daftar Dokumen Prosedur Mutu Bagian TIK

No Dokumen	Prosedur Mutu	Penjelasan
QP-ICT-01	Prosedur Perbaikan Sistem Informasi	Prosedur teknis perbaikan sistem informasi yang telah dikembangkan oleh pihak ketiga
QP-ICT-02	Prosedur Pemeliharaan Perangkat & Infrastruktur Komputer	Prosedur teknis pemeliharaan perangkat keras dan infrastruktur jaringan yang dilakukan setiap semester
QP-ICT-03	Prosedur Penanganan Komplain	Prosedur teknis dalam menangani komplani perangkat keras dan perangkat jaringan
QP-ICT-04	Prosedur Website & Email	Prosedur teknis permintaan unit kerja untuk dibuatkan website dan email STIE Perbanas

No Dokumen	Prosedur Mutu	Penjelasan
QP-ICT-05	Prosedur Video Conference	Prosedur teknis pelaksanaan *video conference* melalui jaringan Inherent
QP-ICT-06	Prosedur Pelaporan EPSBED	Prosedur teknis penyusunan data dan laporan EPSBED
QP-ICT-07	Prosedur Audit Trail	Prosedur teknis audit trail terhadap transaksi data yang tersimpan dalam sistem informasi

Tabel 6. 2 Daftar Dokumen Instruksi Kerja Bagian TIK

No Dokumen	Instruksi Kerja	Penjelasan
WI-ICT-01	Instruksi Kerja Instalasi Jaringan	Instruksi kerja untuk melakukan instalasi jaringan dan koneksi jaringan
WI-ICT-02	Instruksi Kerja Software & Antivirus	Intruksi kerja untuk melakukan instalasi aplikasi atau antivirus pada setiap PC pada unit kerja dengan melalui *master software*
WI-ICT-03	Instruksi Kerja Bandwith Manajemen	Instruksi kerja untuk melakukan pengelolaan dan pengecekan bandwith jaringan
WI-ICT-04	Instruksi Kerja Reset Password User Domain	Instruksi kerja untuk melakukan *reset password* pengguna SISFO
WI-ICT-05	Instruksi Kerja Melihat Password Hotspot User Mahasiswa	Instruksi Kerja untuk melihat *password* mahasiswa melalui alamat IP

WI-ICT-06	Instruksi Kerja Membuat User Hotspot Civitas	Instruksi kerj auntuk menambahkan pengguna pada hostpot
WI-ICT-07	Instruksi Kerja Cek Koneksi Web	Instruksi kerja untuk melakukan pengecekan koneksi website dari luar lingkungan STIE Perbanas
WI-ICT-08	Instruksi Kerja Perbaikan Blue Print TI	Instruksi kerja untuk melakukan perbaikan Blue Print TIK

6.1.1 Hubungan antara Prosedur yang telah ada dan Praktik Keamanan Organisasi

Dalam membangun sebuah prosedur, perlu diperhatikan praktik-praktik keamanan yang telah diimplementasikan dalam organisasi. Tujuan dari memetakan hubungan antara prosedur yang ada dengan praktik keamanan yang telah diimplementasikan oleh organisasi adalah untuk memastikan bahwa prosedur yang ada secara efektif telah mencakup praktik keamanan yang berjalan dalam organisasi. Berdasarkan hasil identifikasi praktik keamanan yang telah dijabarkan dalam bab sebelumnya, maka berikut ini adalah hubungan antara prosedur mutu yang telah diimplementasikan oleh STIE Perbanas dengan praktik keamanan organisasi yang telah berjalan selama ini.

Tabel 6. 3 Hubungan antara Prosedur yang ada dan Praktik Keamanan Organisasi

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
QP-ICT-01	Prosedur Perbaikan Sistem Informasi	• Pelaksanaan SOP terkait mengenai SI/TI di organisasi
QP-ICT-02	Prosedur Pemeliharaan Perangkat &	• Dilakukan maintenance setiap sebelum UTS dan UAS hanya untuk lab saja

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
	Infrastruktur Komputer	• Dilakukan maintenance rutin setiap 6 bulan sekali (diawal semester) untuk kelas dan lab • Dilakukan maintenance Wifi setiap 2 minggu sekali • Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel • Pada Lab tidak bisa menginstall aplikasi dari luar • Pada Lab tidak bisa memasang USB
QP-ICT-03	Prosedur Penanganan Komplain	• Adanya antivirus (e-scan) dan diupdate terus menerus • Adanya update patch dan firewall secara berkala • Telah dipasang anti netcut untuk keamanan Wifi
QP-ICT-04	Prosedur Website & Email	• Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan fungsinya
QP-ICT-05	Prosedur Video Conference	• Pelaksanaan SOP terkait mengenai SI/TI di organisasi
QP-ICT-06	Prosedur Pelaporan EPSBED	• Pelaksanaan SOP terkait mengenai SI/TI di organisasi
QP-ICT-07	Prosedur Audit	• Adanya log setiap aktivitas

No Dokumen	Prosedur Mutu	Praktik Keamanan Organisasi
	Trail	dalam sistem informasi SISFO

6.2 Prosedur yang Dihasilkan dalam Penelitian

Berdasarkan hasil rekomendasi mitigasi risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian. Selain itu, prosedur yang dihasilkan berikut ini juga telah disinkronisasikan dengan prosedur mutu yang ada pada bagian TIK STIE Perbanas Surabaya sehingga telah dapat diverifikasi bahwa tidak ada prosedur yang memiliki fungsi dan proses yang redundan. Berikut ini adalah prosedur yang diusulkan dalam penelitian.

Tabel 6. 4 Prosedur yang Diusulkan

Kontrol Objektif	Prosedur	Pemenuhan Mitigasi Risiko	Ruang Lingkup	Aspek Keamanan
9.1.1 Access Control Policy	Kebijakan Kendali Akses	Sharing password antara mahasiswa/i	Civitas Akademika	Basis data, aplikasi, sistem operasi, file
9.2.1 User Registration and De-registration	SOP Pendaftaran dan Penonaktifan Hak Akses	Username dan password diketahui oleh pengguna lain	Civitas Akademika	Fasilitas email dan internet, SIMAS, E-learning, Perpustakaan, basis data, dan sistem operasi

Kontrol Objektif	Prosedur	Pemenuhan Mitigasi Risiko	Ruang Lingkup	Aspek Keamanan
9.4.3 Password Manajemen Sistem	SOP Manajemen Password		Pengelolaan dan permintaan pergantian password	Fasilitas email dan internet, SIMAS, E-learning, Perpustakaan, basis data, dan sistem operasi
9.1.2 Access to Networks and Network Services	SOP Pendaftaran Akses Jaringan	Terdapat hacker yang memanipulasi data	Civitas Akademika	Fasilitas email dan internet, SIMAS, E-learning, Perpustakaan, basis data, dan sistem operasi

Kontrol Objektif	Prosedur	Pemenuhan Mitigasi Risiko	Ruang Lingkup	Aspek Keamanan
9.4.2 Secure log-on procedure	SOP Secure Log-on	Terdapat hacker yang mencuri data	Pengguna sistem	Aplikasi Server, fasilitas internet, dan aplikasi (SIMAS, E-learning, Perpustakaan)
9.3.1 Use of Secret Authentication Information	Kebijakan Tanggung Jawab Pengguna Teknologi Informasi	Kesalahan dalam pemberian hak akses	Civitas Akademika dan Asosiasi/pihak ketiga	Perangkat komputer dan fasilitas sistem informasi

Berikut ini merupakan penjelasan dari masing-masing prosedur yang akan dibuat untuk mendukung keamanan aset informasi terkait kendali akses pada STIE Perbanas. Jumlah prosedur yang akan dihasilkan adalah sebanyak 4 prosedur dan 2 kebijakan. Penjelasan untuk masing-masing prosedur keterkaitannya dengan proses kekinian akan dijelaskan pada tabel dibawah ini.

Tabel 6. 5 Deskripsi prosedur

Prosedur	Penjelasan
Kebijakan Kendali Akses	Kebijakan kendali akses merupakan kebijakan yang dibuat untuk menjamin persyaratan kendali akses terhadap informasi dan fasilitas sistem informasi (aplikasi, sistem operasi, internet, dan akses ruang server) didefinisikan dengan tepat. Dalam kebijakan ini pun tidak hanya diatur mengenai fasilitas sistem informasi saja, namun juga terkait sumber daya manusia. Beberapa contohnya seperti regulasi penonaktifan hak akses seseorang yang sudah tidak berkepentingan pada organisasi, regulasi pemberian hak akses root, super user, atau administrator kepada seseorang. Kebijakan ini juga bertujuan untuk meminimalisir risiko sharing password antar mahasiswa/mahasiswi karena didalamnya juga mengatur tentang aturan dalam menjaga informasi rahasia yang dimiliki masing-masing civitas akademika.

SOP Pendaftaran dan Penonaktifan Hak Akses	Prosedur pendaftaran dan penonaktifan hak akses merupakan prosedur untuk mengendalikan pendaftaran (registrasi), penghapusan (de-registrati), dan peninjauan hak akses terhadap fasilitas sistem informasi. Pihak-pihak yang wajib mendaftarkan diri agar diberi hak akses terhadap fasilitas sistem informasi adalah seluruh civitas akademika, namun masing-masing elemen tidak akan memiliki hak yang sama. Antara elemen mahasiswa dan dosen akan memiliki kewenangan yang berbeda dalam melakukan akses terhadap fasilitas sistem informasi yang ada di STIE Perbanas. Prosedur ini dibuat juga bertujuan untuk memastikan risiko manipulasi data yang disebabkan oleh username diketahui pengguna lain karena memiliki kesamaan dapat diminimalisir kemungkinan terjadinya.
SOP Manajemen Password	Prosedur manajemen password merupakan prosedur untuk memastikan pengelolaan password telah memenuhi kualitas standard *strong* password. Seluruh sistem informasi yang ada dalam STIE Perbanas yang disebut dengan SISFO mengklasifikasikan penggunanya berdasarkan *login* pengguna pada sistem, sehingga penting untuk memastikan password setiap pengguna telah

	sesuai dengan syarat kualitas password. Prosedur ini juga bertujuan untuk memastikan risiko manipulasi data yang disebabkan oleh password diketahui oleh pengguna lain karena lemahnya kualitas password pengguna dapat diminimalisir kemungkinan terjadinya.
SOP Pendaftaran Akses Jaringan	Prosedur pendaftaran akses jaringan ini merupakan prosedur yang bertujuan untuk menetapkan akses jaringan dan layanan jaringan bagi pengguna sistem sesuai dengan hak aksesnya masing-masing. Prosedur ini berkaitan dengan fasilitas wifi yang tersedia di STIE Perbanas. Hak akses jaringan akan dibedakan dengan adanya prosedur ini, akan ada pembeda akses jaringan dosen dan pegawai, dengan akses jaringan mahasiswa dikarenakan kebutuhan masing-masing elemen berbeda sehingga perlu disesuaikan dengan kebutuhan masing-masing elemen. Dengan adanya pembeda ini diharapkan bisa meminimalisir risiko dari hacker yang ingin memanipulasi data penting yang ada di STIE Perbanas.
SOP Secure Log-on	Prosedur secure log-on ini merupakan prosedur yang bertujuan dalam memberikan rekomendasi pengamanan yang tinggi terhadap aspek autentikasi saat melakukan log in pada sistem maupun aplikasi. Pada prosedur ini berisikan

	mengenai rekomendasi-rekomendasi keamanan yang harus dilakukan agar proses log on yang dilakukan oleh user bisa terjaga kerahasiaannya. Prosedur ini diharapkan bisa meminimalisir risiko pencurian data yang dilakukan oleh hacker dari sisi log on nya.
Kebijakan Tanggung Jawab Pengguna Teknologi Informasi	Kebijakan tanggung jawab pengguna teknologi informasi ini merupakan kebijakan yang dibuat untuk memberikan perlindungan keamanan bagi seluruh civitas akademika di STIE Perbanas ketika menggunakan sumber daya TI atau saat mengakses informasi di STIE Perbanas yang bersifat non-publik. Selain itu kebijakan ini juga memiliki fungsi dalam menerapkan pengamanan yang diperlukan untuk memastikan privasi dari informasi pribadi, ketersediaan informasi dan sumber daya kampus, dan menjaga integritas yang dimiliki STIE Perbanas Surabaya. Diharapkan dengan adanya prosedur ini pemilik informasi pribadi bisa lebih menjaga informasinya sehingga hal-hal terkait penyalahgunaan hak akses bisa diminimalisir.

6.3 Pemetaan SOP yang dihasilkan dengan Prosedur Mutu yang dimiliki STIE Perbanas Surabaya

Pada bagian ini akan dijelaskan mengenai hubungan antara enam prosedur yang dihasilkan dengan *existing procedure* atau prosedur mutu yang telah dimiliki oleh STIE Perbanas. Berdasarkan hasil pembelajaran terhadap prosedur mutu yang telah diimplementasikan, maka terdapat beberapa SOP yang berhubungan dengan prosedur mutu yang ada yaitu SOP Pendaftaran dan Penonaktifan Hak akses dan SOP Akses Jaringan. Sehingga SOP yang dihasilkan akan menjadi dokumen terkait dalam prosedur mutu yang telah ada.

Tabel 6. 6 Hubungan SOP yang diusulkan antara Prosedur Mutu di STIE Perbanas

Prosedur	***Existing Procedure***	**Hubungan dengan *Existing Procedure***
SOP Pendaftaran dan Penonaktifan Hak Akses	Prosedur Website dan Email	Dalam prosedur yang telah ada terdapat prosedur yang menjelaskan mengenai teknis permintaan unit kerja untuk dibuatkan website dan email STIE Perbanas, namun hubungan yang lebih ditekankan disini adalah hubungan saat ingin dibuatkan email. Pembuatan email ini nanti berhubungan dengan SOP Pendaftaran dan Penonaktifan Hak Akses karena username yang digunakan nantinya adalah email yang didaftarkan, hak akses nanti yang akan

		membedakan kewenangan akses dari masing-masing elemen. Dan juga hak akses ini akan dicabut ketika sudah dinonaktifkan yang artinya akses email yang diberikan tidak akan bisa digunakan lagi. Sehingga prosedur ini adalah penyempurna dari prosedur pembuatan website dan email.
SOP Pendaftaran Akses Jaringan	Prosedur Website dan Email	Dalam prosedur yang telah ada terdapat prosedur yang menjelaskan mengenai teknis permintaan unit kerja untuk dibuatkan website dan email STIE Perbanas, namun hubungan yang lebih ditekankan disini adalah hubungan saat ingin dibuatkan email. Email yang dibuat nantinya juga akan dijadikan ID untuk mendaftarkan akses jaringan, sehingga setiap jaringan hanya bisa diakses oleh ID yang sudah didaftarkan ke dalam jaringan tersebut. Jadi ID yang tidak terdaftar dalam jaringan tidak akan bisa mengakses jaringan

		tersebut.

SOP yang diusulkan dalam penelitian ini tidak akan merubah atau bahkan menghapus SOP yang sudah ada, karena SOP yang dihasilkan ini sifatnya mendukung prosedur yang sebelumnya sudah ada di STIE Perbanas. SOP yang diusulkan nanti diharapkan bisa menjadi prosedur pendukung dari prosedur yang sudah ada sebelumnya sehingga prosedur yang diusulkan bisa melengkapi prosedur yang sudah ada.

6.4 Perancangan Struktur dan Isi SOP

Pada sub-bab ini akan dijelaskan mengenai perancangan SOP yang akan dibuat. Perancangan SOP ini mengacu pada peraturan pemerintah (Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia nomor 35 tahun 2012) terkait dengan pedoman penyusunan standard operasioanl prosedur administrasi pemerintah. Namun, dalam perancangan struktur da nisi SOP tidak secara keseluruhan struktur konten akan mengacu pada standard tersebut karena akan disesuaikan dengan kebutuhan. Struktur dokumen SOP yang akan disusun ini akan dihasilkan ke dalam sebuah buku produk yang akan diberikan kepada pihak STIE Perbanas Surabaya sebagai rekomendasi tata kelola keamanan data.

Adapun struktur atau konten yang akan dimasukkan ke dalam kerangkan dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi terkait Kendali Akses STIE Perbanas Surabaya adalah sebagai berikut.

Tabel 6. 7 Hasil Perancangan Dokumen SOP

Struktur Bab	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen SOP Kendali Akses STIE Perbanas
	Ruang Lingkup	
	Overview Kendali Akses	Aspek Kendali Akses

Struktur Bab	Sub-Bab	Konten
	Evaluasi Penilaian Risiko Keamanan Aset Informasi terkait Kendali Akses pada STIE Perbanas	Tabel Daftar Prioritas Risiko Keamanan Aset Informasi terkait Kendali Akses
Kebijakan Kendali Akses	Tujuan	Deskripsi umum kebijakan kendali akses
	Ruang Lingkup	
	Referensi	Referensi kontrol dari standard yang digunakan
	Kebijakan Kendali Akses	Penjelasan mengenai isi kebijakan
Kebijakan Tanggung Jawab Pengguna Teknologi Informasi	Tujuan	Deskripsi umum kebijakan tanggung jawab pengguna teknologi informasi
	Ruang Lingkup	
	Referensi	Referensi kontrol dari standard yang digunakan
	Kebijakan Tanggung Jawab Pengguna Teknologi Informasi	Penjelasan mengenai isi kebijakan
Kebijakan Secure Log-on	Tujuan	Deskripsi umum prosedur
	Ruang Lingkup	
	Referensi	Referensi kontrol dari standard yang digunakan

Struktur Bab	Sub-Bab	Konten
	Kebijakan Secure Log-on	Penjelasan mengenai kebijakan Secure Log-on
Prosedur Pendaftaran dan Penonaktifan Hak Akses	Tujuan	Deskripsi umum prosedur
	Ruang Lingkup	
	Rujukan Standar	Referensi kontrol dari standard yang digunakan
	Prosedur	Pendaftaran/penghapusan hak akses
	Bagan Alur SOP	Tabel bagan alur SOP
	Formulir dan Dokumen Terkait	Formulir User registration dan User De-registration
Prosedur PendaftaranAkses Jaringan	Tujuan	Deskripsi umum prosedur
	Ruang Lingkup	
	Rujukan Standar	Referensi kontrol dari standard yang digunakan
	Prosedur	Prosedur Akses Jaringan
	Bagan Alur SOP	Tabel bagan alur SOP
	Formulir dan Dokumen Terkait	Formulir Akses Jaringan
Prosedur Manajemen Password	Tujuan	Deskripsi umum prosedur
	Ruang Lingkup	
	Rujukan Standar	Referensi kontrol dari standard yang digunakan
	Prosedur	Prosedur Pengelolaan password dan Prosedur Permintaan Pergantian Password
	Bagan Alur	Tabel bagan alur SOP

Struktur Bab	Sub-Bab	Konten
	SOP	
	Formulir dan Dokumen Terkait	Formulir Perbaikan Sistem Informasi dan Formulir Permintaan Pergantian Password
Formulir	Formulir User Registration	
	Formulir User De-registration	
	Formulir Pendaftaran Akses Jaringan	
	Formulir Perbaikan Sistem Informasi	
	Formulir Permintaan Pergantian Password	

6.5 Hasil Perancangan SOP

Pada sub-bab ini akan dijelaskan mengenai hasil akhir dari perencanaan dan perancangan SOP yang telah diinisiasi berdasarkan sub-bab sebelumnya. Tabel dibawah ini akan menampilkan pemetaan dari perancangan SOP dengan formulir yang digunakan pada setiap prosedur maupun kebijakan.

Tabel 6. 8 Pemetaan Dokumen SOP dan Formulir

No Dokumen	Nama Dokumen	No Dokumen	Dokumen Terkait
KJ-KD-01	Kebijakan Kendali Akses		
KJ-KD-02	Kebijakan Tanggung Jawab Pengguna Teknologi Informasi		
KJ-KD-03	Kebijakan Secure Log-on		
PS-01	Prosedur Pendaftaran dan Penonaktifan Hak Akses	FM-01	Formulir User Registration
		FM-02	Formulir User De-registration
PS-02	Prosedur Pendaftaran Akses Jaringan	FM-03	Formulir Pendaftaran Akses Jaringan
PS-03	Prosedur Manajemen Password	FM-04	Formulir Perbaikan Sistem Informasi

No Dokumen	Nama Dokumen	No Dokumen	Dokumen Terkait
		FM-05	Formulir Permintaan Pergantian Password

Berikut adalah penjelasan dari setiap prosedur maupun kebijakan dan formulir beserta dokumen pendukung yaitu formulir yang dibutuhkan pada setiap proses di dalamnya.

6.5.1 Kebijakan Kendali Akses

Sesuai dengan kontrol dalam ISO/IEC:27002:2013 sub klausul 9.1.1 *Access Control Policy*, terdapat beberapa hal yang terkandung di dalamnya yang mengatur mengenai kendali akses yang ditujukan untuk civitas akademika di STIE Perbanas.

II. Kebijakan Kendali Akses

Kebijakan Kendali Akses

KJ-KD-01 Kebijakan Kendali Akses

1. Tujuan

1.1 Kebijakan berikut ini dibuat untuk menjamin persyaratan kendali akses terhadap informasi dan fasilitas sistem informasi (aplikasi, sistem operasi, internet, dan akses ruang Server) didefinisikan dengan tepat

2. Ruang Lingkup

Kebijakan ini berlaku untuk

2.1 Kebijakan ini berlaku untuk pihak-pihak yang terkait dengan pengguna dalam menggunakan sistem informasi dan mejaga keamanan informasi yang berupa data elektronik. Data elektronik yang dimaksud dalam kebijakan meliputi :

- Basis Data
- Aplikasi
- Sistem Operasi
- File

3. Referensi

3.1 ISO/IEC 27002:2013 – A.9.1.1 Access control policy

4. Kebijakan Kendali Akses

4.1 Pemberian hak akses, baik lojik maupun fisik (seperti Ruang Server) harus dibatasi berdasarkan tugas pokok dan fungsi (tupoksi) pengguna dan harus disetujui oleh pembuat keputusan pada bidang yang terkait.

4.2 Tingkatan akses harus diberikan dengan prinsip minimum yang cukup untuk memenuhi kebutuhan pengguna

4.3 Pemberian hak akses yang tingkatannya tinggi (root, super user atau administrator) hanya diberikan kepada karyawan yang benar-benar kompeten, memiliki pengalaman kerja di bagian TI minimum 3 tahun, dan harus disetujui minimum oleh pembuat keputusan pada bidang yang terkait.

4.4 Hak akses pengguna di STIE Perbanas yang statusnya tertera dibawah ini harus segera di non-aktifkan maksimum 7 hari setelah tanggal yang ditetapkan :

- Mahasiswa :
  - Lulus dari program studi
  - Gagal untuk melakukan re-enrol selama masa program studi
  - Dikeluarkan dari STIE Perbanas
- Staf:
  - Memutuskan hubungan kerja
  - Mengundurkan diri

- Pensiun
- Asosiasi (Pihak ketiga):
  - Kontrak kerja sama sudah habis

4.5 Hak akses tidak boleh dipinjamkan kepada pengguna lain.

4.6 Seluruh hak akses pengguna akan direview setiap 6 bulan sekali.

4.7 Tata cara pendaftaran, dan penutupan hak akses diatur dalam Prosedur Pendaftaran dan Penonaktifan Hak Akses.

4.8 Setiap pengecualian terhadap kebijakan ini hanya dapat dilakukan atas persetujuan pembuat keputusan pada bidang yang terkait.

4.9 Akses Pihak Ketiga

4.9.1 Vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses fisik atau lojik ke dalam aset STIE Perbanas harus menandatangani Ketentuan/Persyaratan Menjaga Kerahasiaan Informasi

4.9.2 Hak akses pihak ketiga hanya diberikan berdasarkan kepentingan STIE Perbanas yang disahkan melalui kerjasama atau kontrak

4.9.3 Seluruh hak akses pihak ketiga harus dibatasi waktunya, dicatat, dan ditinjau penggunaannya (log).

4.9.4 Seluruh akses yang disediakan bagi pelanggan STIE Perbanas harus mematuhi kebijakan keamanan informasi.

4.9.5 Seluruh koneksi pihak ketiga ke dalam network STIE Perbanas harus dibatasi hanya terhadap host dan/atau aplikasi tertentu yang ditetapkan oleh Departemen TI

4.10 Pengelolaan Password

4.10.1 Password minimum terdiri dari 8 karakter kombinasi angka dan huruf serta tidak boleh menggunakan karakter yang mudah ditebak.

4.10.2 Pengguna harus mengganti *default password* yang diberikan saat pertama kali mendapatkan hak akses.

4.10.3 *Password* tidak boleh :

- *Diberitahukan kepada orang lain*
- *Ditulis di media yang mudah terlihat orang lain*

4.10.4 *Password* diganti secara berkala atau segera diganti bila diduga telah diketahui orang lain. Periode penggantian *password*:

- *Untuk pengguna biasa (seperti: email, web, komputer) minimum setiap 180 hari*
- *Untuk pengguna sistem (seperti: root, admin server/aplikasi) minimum setiap 60 hari*

4.10.5 Seluruh *default password* dan password dari vendor harus diganti segera setelah instalasi selesai atau sistem diserahkan ke STIE Perbanas.

4.10.6 Hak akses akan direset atau dinonaktifkan jika tidak pernah digunakan selama 90 hari secara berturut-turut. Untuk mengaktifkannya kembali, pengguna harus mengajukan pendaftaran kembali sesuai Prosedur Pengendalian Hak Akses.

4.11 Kebijakan kendali akses ini harus didukung dengan kebijakan tanggung jawab pengguna teknologi informasi

Gambar 6. 1 Kebijakan Kendali Akses

6.5.2 Kebijakan Tanggung Jawab Pengguna Teknologi Informasi

Sesuai dengan kontrol dalam ISO/IEC:27002:2013 sub klausul 9.3.1 *Use of Secrets Authentication Information*, terdapat beberapa hal yang terkandung di dalamnya yang mengatur mengenai tanggung jawab pengguna teknologi informasi yang ditujukan untuk civitas akademika di STIE Perbanas.

Kebijakan Tanggung Jawab Pengguna Teknologi Informasi

KJ-KD-02 Kebijakan Tanggung Jawab Pengguna Teknologi Informasi

1. Tujuan

1.1 Kebijakan ini dibuat untuk memberikan perlindungan keamanan bagi seluruh civitas akademika di STIE Perbanas ketika menggunakan sumber daya TI atau saat mengakses informasi di STIE Perbanas yang bersifat non-publik.

1.2 Menerapkan pengamanan yang diperlukan untuk memastikan privasi dari informasi pribadi, ketersediaan informasi dan sumber daya kampus, dan menjaga integritas yang dimiliki STIE Perbanas.

2. Ruang Lingkup

Kebijakan ini berlaku untuk

2.1 Kebijakan ini berlaku untuk pengguna yang menggunakan seluruh fasilitias sistem informasi yang ada di STIE Perbanas. Pengguna yang dimaksudkan tersebut antara lain :

- Mahasiswa STIE Perbanas
- Pegawai STIE Perbanas
- Asosiasi / Pihak Ketiga

3. Referensi

3.1 ISO/IEC 27002:2013 – A.9.3.1 Use of Secrets Authentication Information

4. Kebijakan Tanggung Jawab Pengguna Teknologi Informasi

4.1 Hal ini merupakan tanggung jawab setiap pengguna sumber daya TI untuk mengetahui persyaratan keamanan kampus dan melakukannya dengan sesuai. Pengguna sumber daya TI harus memenuhi persyaratan sebagai berikut:

4.1.1 **Menghormati dan melindungi privasi orang lain.** Pengguna harus menghormati privasi orang lain ketika berhadapan dengan informasi yang bersifat pribadi dan harus mengambil tindakan pencegahan yang tepat untuk melindungi informasi tersebut dari penggunaan oleh orang yang tidak berwenang.

4.1.2 **Jangan menyimpan informasi rahasia di Workstation dan Perangkat Mobile, kecuali ketika sangat dibutuhkan untuk tujuan bisnis.** Informasi yang sifatnya rahasia tidak seharusnya disimpan di workstation dan perangkat mobile (laptop, flashdisk, dsb.) kecuali khusus dan dibenarkan untuk tujuan bisnis dan keamanannya bisa dijamin. Jika informasi rahasia tersebut disimpan memang terpaksa harus disimpan pada workstation atau perangkat mobile, pengguna harus melakukan enkripsi terhadap informasi tersebut untuk melindungi informasi agar tidak dibuka oleh pihak yang tidak berwenang.

4.1.3 **Menjaga kebersihan meja dan kebersihan layar komputer.** Maksud dari kebersihan disini adalah bersih dari data dan informasi rahasia, pengguna harus menjaga informasi rahasia agar tidak muncul dan berserakan di tempat yang mudah dilihat oleh publik dan pengguna tidak boleh meninggalkan informasi dalam keadaan terbuka ketika informasi tersebut sudah tidak dibutuhkan/digunakan.

4.1.4 **Lindungi workstation dan perangkat komputer yang lain.** Pengguna sumberdaya TI harus bertanggung jawab untuk membantu mengelola keamanan dari workstation dan perangkat komputer yang lain untuk melindungi perangkat informasi-informasi yang ada di dalamnya dari akses oleh orang-orang yang tidak berwenang dan infeksi terhdapat perangkat lunak yang berbahaya (virus, worm dan spyware).

4.1.5 **Melindungi Password.** Password biasanya digunakan untuk membuktikan identitas seseorang dan mendapatkan akses ke sebuah perangkat. Setiap civitas akademika bertanggung jawab untuk melindungi password yang dimiliki dan tidak membagikannya dengan orang lain.

4.1.6 **Melaporkan pelanggaran, malfungsi, dan kelemahan keamanan.** Pengguna sumber daya TI harus melaporkan jika menemukan pelanggaran yang berkaitan dengan keamanan TI, atau menemukan kesalahan dan kelemahan dari sistem keamanan yang dimiliki oleh STIE Perbanas.

4.1.7 **Memanfaatkan informasi kampus dan sumber daya TI hanya untuk keperluan resmi saja.** Pengguna sumber daya TI seharunya menggunakan dan memanfaatkan informasi dan sumber daya TI yang dimiliki kampus hanya untuk keperluan yang bersangkutan dengan kampus saja dan sifatnya resmi, bukan digunakan untuk hal-hal yang sifatnya untuk kepentingan pribadi semata, terlebih lagi untuk hal-hal yang bisa merugikan civitas akademika di perbanas dan STIE Perbanas itu sendiri.

4.2 Pelatihan Keamanan Teknologi Informasi diperlukan untuk pengguna IT

4.2.1 Seluruh pengguna TI yang memiliki akses terhadap sumber daya teknologi informasi akan diminta untuk mengikuti Pelatihan Keamanan Teknologi Informasi sebelum menerima akses dan pelatihan dilaksanakan setiap tahun.

Gambar 6. 2 Kebijakan Tanggung Jawab Pengguna Teknologi Informasi

6.5.3 Kebijakan Secure Log-on

Prosedur ini menjelaskan mengenai langkah-langkah dalam melakukan proses mengamankan fase log on pada sebuah web atau aplikasi sesuai dengan kontrol pada ISO/IEC:27002:2013 pada sub klausul 9.4.2 *Secure Log-on Procedures*. Berikut ini adalah prosedur dari secure log-on.

Kebijakan Secure Log-on

KJ-KD-03 Secure Log-on

1. Tujuan

1.1. Tujuan dari prosedur ini adalah memberikan rekomendasi pengamanan yang tinggi terhadap aspek autentikasi saat melakukan log in pada sistem maupun aplikasi

1.2. Mencegah akses tidak sah ke dalam sistem dan aplikasi

2. Ruang Lingkup

Prosedur ini berlaku untuk akses terhadap :

2.2 Log-on Aplikasi Server

2.3 Log-on Fasilitas Internet

2.4 Log-on Aplikasi (SIMAS, E-learning, Perpustakaan)

3. Rujukan Standar

3.1. ISO/IEC 27002:2013 Sub Klausul A.9.4.2 Secure log-on procedures

4. Prosedur

4.1 Prosedur Secure Log-on

4.1.1 Tidak menampilkan pengidentifikasi sistem atau aplikasi sampai proses log-on sudah berhasil dan selesai.

4.1.2 Menampilkan peringatan pemberitahuan umum bahwa komputer hanya bisa diakses oleh pengguna yang berwenang.

4.1.3 Tidak menyediakan pesan bantuan selama prosedur secure log-on berlangsung yang bisa memberikan bantuan kepada pengguna yang tidak berwenang.

4.1.4 Validasi informasi log-on hanya jika seluruh data yang dibutuhkan diisi secara lengkap dan benar. Jika sebuah kondisi error muncul, sistem tidak boleh menunjukkan bagian data mana yang benar dan yang salah.

4.1.5 Batasi jumlah kesempatan log-on gagal yang diizinkan.

4.1.6 Catat berapa kali yang gagal dan berhasil.

4.1.7 Membuat penundaan waktu sebelum upaya log on lanjut diperbolehkan.

4.1.8 Kirim sebuah pesan pengingat jika jumlah maksimal dari upaya login sudah habis.

4.1.9 Tampilkan informasi berikut ini pada saat log on berhasil :

- Tanggal dan waktu dari log on yang sukses dilakukan sebelumnya
- Detail dari semua upaya log on yang tidak berhasil sejak terakhir kali log on berhasil dilakukan

4.1.10 Tidak menampilkan password yang dimasukkan atau sembunyikan karakter password dengan menggunakan simbol.

4.1.11 Tidak mengirimkan password dalam bentuk teks melalui jaringan

Gambar 6. 3 .Kebijakan Secure Log-on

6.5.4 Prosedur Pendaftaran dan Penonaktifan Hak Akses

Prosedur ini menjelaskan mengenai langkah-langkah dalam melakukan pendaftaran dan penonaktifan *User ID* sesuai dengan kontrol pada ISO/IEC:27002:2013 pada sub klausul

9.2.1 *User registration and de-registgration*. Berikut ini adalah prosedur dari pendaftaran dan penonaktifan hak akses.

Pendaftaran dan Penonaktifan Hak Akses

PS-01 Pendaftaran dan Penontaktifan Hak Akses

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	PS-01	NO. RILIS :
		NO. REVISI :
	PROSEDUR PENDAFTARAN DAN PENONAKTIFAN HAK AKSES	TANGGAL TERBIT :
		HALAMAN :
PROSEDUR		

1. Tujuan

1.1 Tujuan dari prosedur ini adalah mengendalikan pendaftaran (registrasi), penghapusan (de-registrasi), dan peninjauan hak akses terhadap ruang Server dan sistem informasi

1.2 Mencegah agar hak akses hanya diberikan kepada karyawan yang berwenang

2. Ruang Lingkup

Prosedur ini berlaku untuk akses terhadap :

2.1 Fasilitas email dan Internet

2.2 Aplikasi (SIMAS, E-learning, Perpustakaan), basis data, dan sistem operasi

3. Rujukan Standar

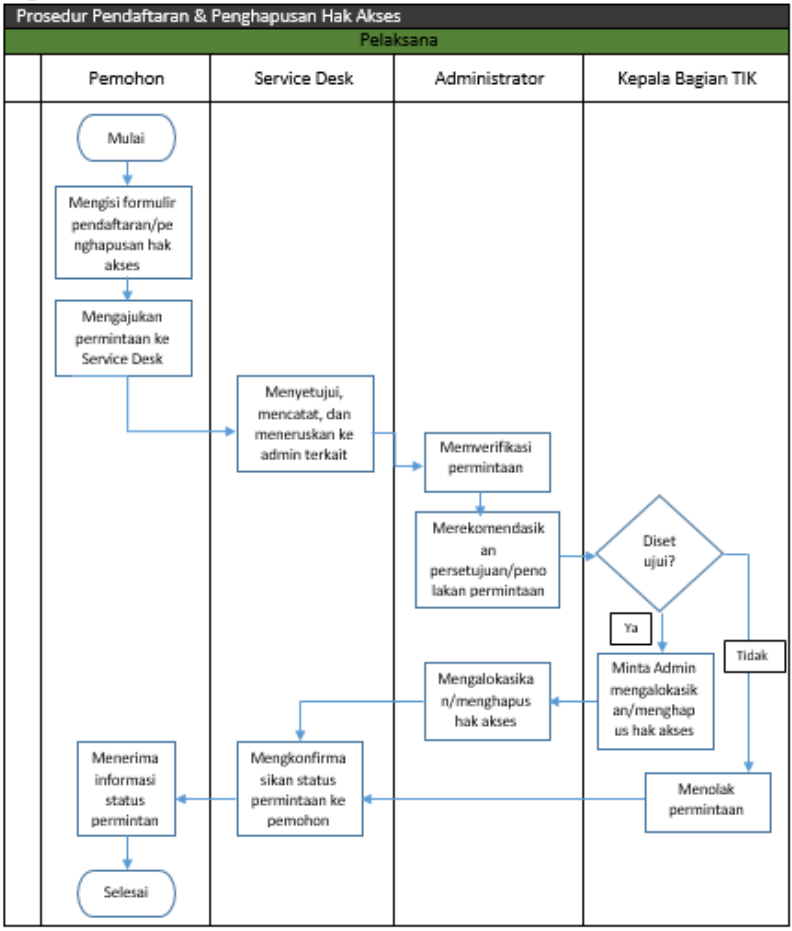
3.1 ISO/IEC 27002:2013 Sub Klausul A.9.2.1 User registration and de-registration

4. Prosedur

4.1 Pendaftaran/Penghapusan Hak Akses

Gambar 6. 4 Prosedur Pendaftaran dan Penonaktifan Hak Akses

Bagan Alur SOP – Pendaftaran dan Penonaktifan Hak Akses



Gambar 6. 5 Bagan alur SOP

6.5.5 Prosedur Pendaftaran Akses Jaringan

Pada prosedur ini akan dibahas mengenai langkah-langkah dalam meminta akses jaringan kepada bagian staff TIK. Proses ini penting sebagai upaya untuk membedakan jaringan dan layanan yang bisa diakses oleh elemen yang berbeda. Prosedur ini telah disesuaikan dengan kontrol yang ada pada ISO/IEC:27002:2013 sub-klausul 9.1.2 *Access to networks and network services*. Berikut ini merupakan prosedur dari akses jaringan beserta langkah-langkahnya.

Pendaftaran Akses Jaringan

PS-02 Pendaftaran Akses Jaringan

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	PS-03	NO. RILIS : NO. REVISI :
	PROSEDUR PENDAFTARAN AKSES JARINGAN	TANGGAL TERBIT : HALAMAN :
PROSEDUR		

1. Tujuan

1.1 Tujuan dari prosedur ini adalah menetapkan akses jaringan dan layanan jaringan bagi pengguna sistem sesuai dengan hak aksesnya masing-masing

2. Ruang Lingkup

Prosedur ini berlaku terhadap :

2.1 Mahasiswa STIE Perbanas

2.2 Staff STIE Perbanas

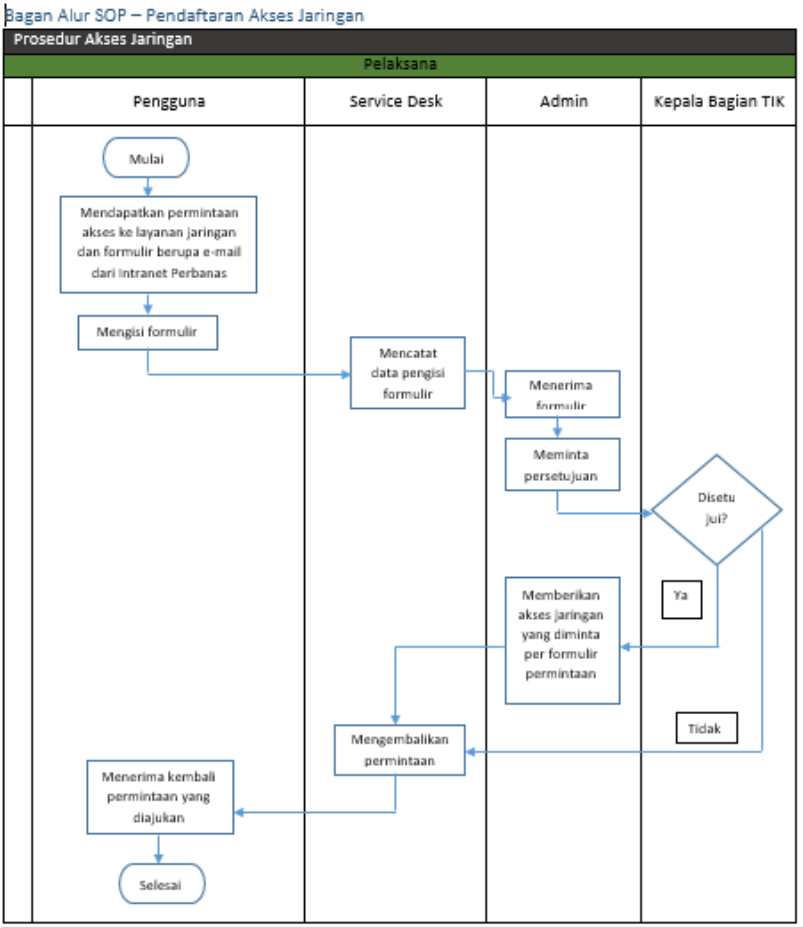
3. Rujukan Standar

3.1 ISO/IEC 27002:2013 Sub Klausul A.9.1.2 Access to networks and network services

4. Prosedur

4.1 Prosedur Pendaftaran Akses Jaringan

Gambar 6. 6 SOP Pendaftaran Akses Jaringan



Gambar 6. 7 Bagan Alur SOP Pendaftaran Akses Jaringan

6.5.6 Prosedur Manajemen Password

Sesuai dengan kontrol dalam ISO/IEC:27002:2013 pada sub klausul 9.4.3 *Password management system*, prosedur ini berisi 2 proses utama yang didefinisikan dalam beberapa aktivitas yang berurutan.

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	PS-03	NO. RILIS :
		NO. REVISI :
	PROSEDUR MANAJEMEN PASSWORD	TANGGAL TERBIT :
		HALAMAN :
PROSEDUR		

1. Tujuan

1.1 Tujuan dari prosedur ini adalah untuk memastikan pengelolaan password telah memenuhi kualitas standard *strong password*.

2. Ruang Lingkup

Prosedur ini mencakup proses pengelolaan penggunaan password yang meliputi :

2.1 Proses pengelolaan password

2.2 Proses permintaan pergantian password

3. Rujukan Standar

3.1 ISO/IEC 27002:2013 Sub Klausul A.9.4.3 Password management system

4. Prosedur

4.1 Proses pengelolaan password

4.1.1 Kepala Bagian TIK menentukan standar penggunaan *password* sesuai dengan kualitas standard *strong password* yang tercantum dalam Kebijakan Pengendalian Hak Akses pada sub Pengelolaan Password.

4.1.2 Kepala Bagian TIK menginstruksikan kepada Staff TIK (administrator apliaksi) untuk melakukan penambahan fitur *strong password* dalam sistem informasi.

4.1.3 Staff TIK menganalisis kebutuhan sistem informasi untuk penambahan fitur *strong password* dan menentukan waktu pengerjaan.

4.1.4 Staff TIK (administrator aplikasi) mengerjakan penambahan fitur *strong password* sesuai dengan waktu yang ditentukan.

4.1.5 Staff TIK memastikan seluruh sistem informasi yang membutuhkan prosedur log on telah memiliki ketentuan inputan *strong password*.

4.1.6 Staff TIK melakukan pengujian terhadap fitur baru *strong password*

a. Uji coba berhasil

- Staff TIK lalu melakukan pelaporan kepada Kepala Bagian TIK.

- Kepala Bagian TIK melakukan validasi dan persetujuan hasil penambahan fitur.
- Staff TIK kemudian mengisi laporan perbaikan fitur pada sistem informasi pada formulir Perbaikan Sistem Informasi.

b. Uji coba gagal

- Staff TIK melakukan kembali prosedur pada sub proses 4.1.3

4.1.7 Staff TIK kemudian melakukan pelaporan pembaharuan fitur pada sistem informasi dengan mengisi formulir Perbaikan Sistem Informasi.

4.1.8 Staff TIK mempersiapkan prosedur perubahan *password* lama dan melakukan *setup* pada seluruh sistem.

4.1.9 Sistem menyediakan *password default* sementara yang telah sesuai dengan standar *strong password* untuk masing-masing pengguna sistem.

4.1.10 Staff mensosialisasikan penambahan fitur baru kepada seluruh civitas akademika melalui website resmi.

4.1.11 Staff TIK mengirimkan *e-mail* yang berisikan *password default* sementara untuk seluruh pengguna sistem dan informasi mengenai ketentuan penggunaan kualitas standard *strong password*.

4.1.12 Pengguna sistem kemudian harus melakukan *login* dengan menggunakan *password default*.

4.1.13 Sistem selanjutnya menampilkan notifikasi untuk meminta civitas akademika melakukan pergantian *password default* dengan *password* baru yang sesuai dengan ketentuan kualitas standard *strong password*.

4.1.14 Staff TIK memastikan seluruh civitas akademika telah mengganti *password default* dalam kurun waktu kurang dari satu bulan.

4.1.15 Staff TIK mengelola data penggunaan *password* lama dan memastikan tidak ada penggunaan kembali *password default*.

4.2 Proses permintaan pergantian password

4.2.1 Pengguna sistem melakukan permintaan pergantian *password* dengan mengisi formulir permintaan pergantian *password* dengan menyertakan alasan permintaan pergantian *password*.

4.2.2 Staff TIK melakukan validasi permintaan.

4.2.3 Staff TIK kemudian mengirimkan *e-mail* yang berisikan *link* untuk menginputkan *password* baru kepada pengguna sistem yang melakukan permintaan pergantian *password*.

4.2.4 Pengguna sistem kemudian mengakses *link* dan menginputkan *password* baru.

4.2.5 Sistem selanjutnya melakukan verifikasi dan validasi inputan *password* baru.

5. Formulir dan Dokumen Terkait

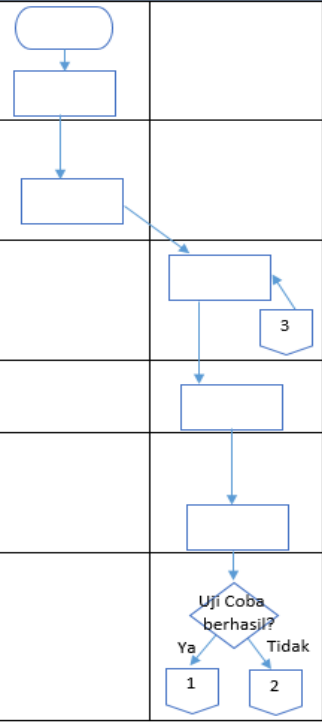
Prosedur ini memiliki formulir atau dokumen terkait yang meliputi :

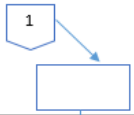
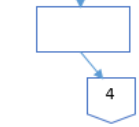
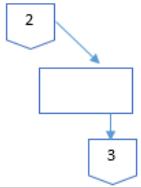
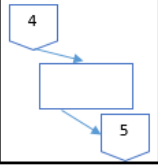
5.1 Formulir Perbaikan Sistem Informasi

5.2 Formulir Permintaan Pergantian Password

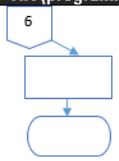
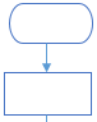
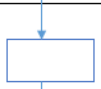
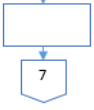
Gambar 6. 8 Prosedur Manajemen Password

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.	Proses Pengelolaan Password					
1.1	Menentukan standar penggunaan password sesuai dengan kualitas standard *strong password*					KJ-03 Kebijakan Penggunaan Akun dan Kata Sandi
1.2	Menginstruksikan kepada Pegawai Bagian TIK (administrator aplikasi) untuk melakukan penambahan fitur *strong password* dalam sistem informasi					
1.3	Menganalisis kebutuhan sistem informasi untuk penambahan fitur *strong password* dan menentukan waktu pengerjaan					
1.4	Mengerjakan penambahan fitur *strong password* sesuai dengan waktu yang ditentukan					
1.5	Memastikan seluruh sistem informasi yang membutuhkan prosedur *log in* telah memiliki ketentuan inputan *strong password*					
1.6	Melakukan pengujian terhadap fitur baru *strong password*					



	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
a.1	**Uji coba berhasil** Melakukan pelaporan kepada Kepala Bagian TIK					
a.2	Melakukan validasi dan persetujuan hasil penambahan fitur					
a.3	Mengisi laporan perbaikan fitur pada sistem informasi pada formulir Perbaikan Sistem Informasi					FM – 01 Formulir Perbaikan Sistem Informasi
b.1	**Uji coba gagal** Melakukakan kembali melakukan prosedur pada sub proses 1.3					
1.7	Mempersiapkan prosedur perubahan *password* lama dan melakukan *set up* pada seluruh sistem					

	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.8	Menyediakan *password default* sementara untuk masing pengguna sistem		5			
1.9	Mensosialisasikan penambahan fitur baru kepada seluruh civitas akademika melalui website resmi					
1.10	Mengirimkan *email* yang berisikan *password default* sementara untuk seluruh civitas akademika mengenai ketentuan penggunaan *strong password*					
1.11	Melakukan *login* dengan menggunakan *password default*					
1.12	Mengeluarkan notifikasi untuk melakukan pergantian *password default* dengan password baru yang sesuai dengan ketentuan kualitas standard *strong password*					
1.13	Memastikan seluruh civitas akademika mengganti *password default* dalam kurun waktu selama satu bulan		6			

	URAIAN PROSEDUR	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
1.14	Mengelola data penggunaan password lama dan memastikan tidak ada penggunaan kembali *password default*					
2. Proses Permintaan pergantian password						
2.1	Melakukan permintaan pergantian password					
a.1	**Mahasiswa** Mengajukan permintaan pergantian password dengan mengisi formulir permintaan pergantian password					
a.2	Mengisikan formulir permintaan pergantian password dan menyertakan alasan pengajuan permintaan password					FM-01 Formulir Permintaan Pergantian Password
2.2	Melakukan validasi pada formulir permintaan pergantian password					FM-01 Formulir Permintaan Pergantian Password

	URAIAN PROSEDUR	PELAKSANA				DOKUMEN TERKAIT
		Kepala Bagian TIK	Pegawai Bagian TIK (programmer)	Pengguna Sistem	Sistem	
2.3	Mengirimkan *email* yang berisikan link untuk menginputkan password baru kepada civitas akademika yang melakukan permintaan pergantian password		7			
2.4	Mengakses *link* dan menginputkan *password* baru					
2.5	Melakukan verifikasi dan validasi inputan password baru					

Gambar 6. 9 Alur bagan SOP Manajemen Password

6.5.7 Formulir

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan setiap aktivitas dengan baik. Berikut adalah 5 formulir yang dibutuhkan untuk mendukung pelaksanaan SOP.

6.5.7.1 Formulir User Registration

Formulir user registration adalah usulan formulir yang dapat digunakan oleh seluruh civitas akademika untuk mendokumentasikan setiap pendaftaran hak akses (User ID) untuk melakukan akses pada fasilitas sistem informasi di STIE Perbanas Surabaya. Formulir yang dibuat dibedakan menjadi dua kategori yaitu formulir permintaan pergantian password untuk pegawai (dosen dan pegawai) dan juga untuk mahasiswa. Formulir user registration dapat dilihat pada lampiran F.

6.5.7.2 Formulir User De-registration

Formulir user de-registration adalah usulan formulir yang dapat digunakan oleh seluruh civitas akademika untuk mendokumentasikan setiap penonaktifan hak akses (User ID) yang telah digunakan untuk melakukan akses pada fasilitias sistem informasi di STIE Perbanas Surabaya. Formulir yang dibuat dibedakan menjadi dua kategori yaitu formulir permintaan pergantian password untuk pegawai (dosen dan pegawai) dan juga untuk mahasiswa. Formulir user de-registration dapat dilihat pada lampiran F

6.5.7.3 Formulir Pendaftaran Akses Jaringan

Formulir Pendaftaran Akses jaringan adalah usulan formulir yang dapat digunakan oleh seluruh civitas akademika untuk mendokumentasikan setiap permintaan akses jaringan yang akan digunakan untuk mengakses fasilitas sistem informasi di STIE Perbanas Surabaya sesuai dengan kewenangan dan hak masing-masing elemen. Formulir yang dibuat dibedakan menjadi dua kategori yaitu formulir permintaan pergantian password untuk pegawai (dosen dan pegawai) dan juga untuk

mahasiswa. Formulir pendaftaran akses jaringan dapat dilihat pada lampiran F.

6.5.7.4 Formulir Perbaikan Sistem Informasi

Formulir perbaikan sistem informasi adalah usulan formulir yang dapat digunakan oleh Bagian TIK untuk mendokumentasikan setiap penambahan fitur maupun perubahan dan perbaikan yang dilakukan pada sistem informasi yang dikelola. Formulir perbaikan sistem informasi dapat dilihat pada lampiran F.

6.5.7.5 Formulir Permintaan Pergantian Password

Formulir permintaan pergantian password adalah usulan formulir yang dapat digunakan seluruh civitas akademika untuk mengajukan permintaan pergantian password apabila pengguna merasa bahwa terdapat indikasi informasi mengenai password telah diketahui pihak lain. Formulir yang dibuat dibedakan menjadi dua kategori yaitu formulir permintaan pergantian password untuk pegawai (dosen dan pegawai) dan juga untuk mahasiswa. Formulir permintaan pergantian password terlampir pada lampiran F.

6.6 Hasil Pengujian SOP

Pengujian SOP dilakukan dengan verifikasi dan validasi. Verifikasi dilakukan dengan wawancara untuk memastikan kesesuaian antara prosedur yang dihasilkan dengan kebutuhan STIE Perbanas. Sementara validasi dilakukan dengan cara mensimulasikan SOP untuk mengetahui ketepatan prosedur ketika diimplementasikan dalam kasus yang nyata.

6.6.1 Hasil Verifikasi

Verifikasi SOP dilakukan dengan cara wawancara pada Kasie Bagian TIK yang hasilnya secara detail akan dilampirkan pada Lampiran G. Dari hasil verifikasi, dibutuhkan beberapa revisi dokumen SOP, yaitu :

1. **Perubahan Formulir User Registration**
   Setelah melakukan verifikasi, Kasie Bagian TIK melakukan koreksi pada formulir user registration. Kasie Bagian TIK meminta untuk menambahkan beberapa field. Sehingga perubahan yang dilakukan dapat dilihat pada gambar berikut :

- Sebelum Perubahan

FORMULIR USER REGISTRATION
Nomor FM-01 - ... / ... / ...

Pemohon	
Nama :	Tanda Tangan :
NRP :	
Angkatan :	
Fakultas :	
Jurusan :	
Email Aktif :	
Tanggal :	
	(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar 6. 10 Formulir User Registration Sebelum Perubahan

- Setelah Perubahan

FORMULIR USER REGISTRATION
Nomor FM-01 - ... / ... / ...

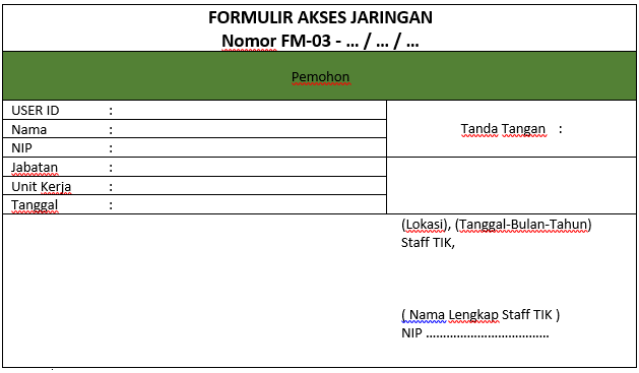
Pemohon	
Nama :	Tanda Tangan :
NRP :	
Angkatan :	
Fakultas :	
Jurusan :	
Email Aktif :	
Tanggal :	
Buat Baru : ☐ Ya ☐ Tidak	
Alasan Ganti :	
	(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar 6. 11 Formulir User Registration Setelah Perubahan

2. Perubahan Formulir Pendaftaran Akses Jaringan

Setelah melakukan verifikasi, Kasie Bagian TIK melakukan koreksi pada formulir akses jaringan. Kasie Bagian TIK meminta penambahan beberapa field yaitu field Daftar Wifi dan Daftar Layanan. Sehingga perubahan dari formulir bisa dilihat pada gambar berikut ini :

- Sebelum Perubahan



FORMULIR AKSES JARINGAN
Nomor FM-03 - ... / ... / ...

Pemohon	
USER ID :	Tanda Tangan :
Nama :	
NIP :	
Jabatan :	
Unit Kerja :	
Tanggal :	
	(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar 6. 12 Formulir Pendaftaran Akses Jaringan Sebelum Perubahan

- Setelah Perubahan

FORMULIR PENDAFTARAN AKSES JARINGAN
Nomor FM-03 - ... / ... / ...

Pemohon	
USER ID : bagus@perbanas.ac.id	Tanda Tangan :
Nama : bagus prasetyo	
NIP : 123452214551	
Jabatan : Kepala Bagian Kepegawaian	
Unit Kerja : Kepegawaian	
Daftar Wifi : (Diisi oleh staff)	
Daftar Layanan : (Diisi oleh staff)	
Tanggal : DDMMYYYY	
	(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar 6. 13 Formulir Pendaftaran Akses Jaringan Sebelum Perubahan

6.6.2 Hasil Validasi

Validasi SOP dilakukan dengan mensimulasikan beberapa aktivitas operasional yang benar-benar terjadi. Berikut adalah pemetaan antara masing-masing prosedur dan skenario simulasinya yang dijelaskan dalam tabel dibawah ini.

Tabel 6. 9 Hasil Validasi

No	SOP	Skenario	Tanggal	Keterangan
1.	SOP Pendaftaran dan Penonaktifan Hak Akses	Salah satu mahasiswa melakukan permintaan pendaftaran hak akses. Sebelumnya mahasiswa diberi email baru untuk melakukan pendaftaran hak akses baru.	4 Januari 2016	Pada SOP ini hanya dilakukan pendaftaran hak akses saja karena proses penonaktifan hak akses dan pendaftaran sama dan juga hanya dilakukan pendaftaran untuk mahasiswa sehingga dengan pertimbangan bisa mengefisiensi waktu dan juga terkendala kepadatan kegiatan divisi TIK STIE

No	SOP	Skenario	Tanggal	Keterangan
				Perbanas.
2.	SOP Pendaftaran Akses Jaringan	Mahasiswa yang sudah mendapatkan hak aksesnya tadi mengajukan permintaan untuk mendapatkan akses wifi dan layanan sistem informasi sesuai dengan statusnya.	4 Januari 2016	Formulir yang digunakan adalah formulir untuk mahasiswa saja, tidak dilakukan validasi formulir untuk pegawai
3.	SOP Manajemen Password	Kasie TIK meminta programmer untuk menambahkan fitur *strong password* pada sistem informasi kepegawaian dan salah satu mahasiswa yaitu	4 Januari 2016	Dilakukan dengan baik

No	SOP	Skenario	Tanggal	Keterangan
		Bagus Prasojo melakukan permiintaan pergantian *password*		

(halaman ini sengaja dikosongkan)

LAMPIRAN A : HASIL WAWANCARA DENGAN PEMBANTU KETUA BIDANG AKADEMIK STIE PERBANAS

Berikut ini adalah lampiran dokumen dari penelitian ini.

I. Informasi Interview 1

- Nama Narasumber : Dr. Drs. Emanuel Kritijadi, MM
- Jabatan : Pembantu Ketua Bidang Akademik
- Jenis Kelamin : Laki-Laki
- Tanggal dan Waktu : 4 Nopember 2015

A. Informasi Narasumber

1. Apakah peran dan tanggung jawab anda sebagai Pembantu Ketua Bidang Akademik?
   Mengelola pelaksanaan rencana strategis bidang pendidikan dan pengajaran serta menyusun dan mengusulkan kepada ketua STIE Perbanas mengenai sistem dan peraturan/ketentuan bidang akademik, pengembangan metode dan evaluasi pengajaran, sistem penjaminan kualitas pendidikan, pembinaan dan pengembangan jurusan dan program diploma, pengelolaan data untuk kepentingan akreditasi dan laporan bidang akademik.
2. Apa sajakah aktivitas utama dalam proses bisnis Perbanas?
   Secara keseluruhan aktvitas utama terdiri dari proses utama yaitu penerimaan mahasiswa → kegiatan harmoni → FRS → Perkuliahan → UTS → UAS → (*magang untuk D3*) →Tugas Akhir → Yudisium → Wisuda.

B. Pertanyaan mengenai Keamanan Aset Informasi terkait Kendali Akses

Tabel A. 1 Hasil wawancara keamanan aset informasi terkait kendali akses

Pertanyaan Identifikasi	Jawaban Narasumber
1. Menurut anda, apa sajakah data dan aset yang kritikal dan sensitive dalam operasional di STIE Perbanas?	Data yang paling kritikal ada dua yaitu data demografi dan data akademik. Data demografi adalah data data seperti data mahasiswa termasuk data seperti nama, alamat, riwayat pendidikan, presetasi dan lainnya sedangkan data akademik yaitu data nilai perkuliahan, IPK dan lainnya. Sedangkan aset yang kritikal yaitu server, PC, dan yang kritis ini adalah mahasiswa.
2. Siapa saja yang memiliki hak akses terhadap data dan aset yang kritikal dan sensitive yang disebutkan diatas?	Mahasiswa memiliki akses terhadap masing masing data demografinya namun hanya pada batas dapat melihat dan tidak dapat melakukan perubahan terhadap data tersebut. Hal itu dikarenakan sesuai dengan kebijakan bahwa mahsiswa dibatasi atas perubahan data agar data yang di inputkan sejak mahasiswa diterima hingga kelulusan tetap sama, dan apabila mahasiswa akan melakukan perubahan maka harus melalui prosedur terlebih dahulu. Sedangkan untuk data akademik seperti nilai setiap dosen akan menginputkan nilai pada batas waktu yang ditentukan dan jika lewat dari batas waktu tersebut maka dosen dapat melakukan perubahan dengan melalui prosedur terlebih dahulu dan atas sepengatahun bidang akademik. Mahasiswa dapat melihat nilainya melalui sistem informasi akademik

Pertanyaan Identifikasi	Jawaban Narasumber
	mahasiswa dengan terlebih dahulu melakukan login dengan username dan password.
3. Apa saja praktek pengamanan yang telah dilakukan oleh STIE Perbanas terhadap data dan aset yang kritikal dan sensitive yang disebutkan diatas?	Seperti penggunaan username dan password untuk setiap akses pada sistem informasi akademik, kemudian adanya batasan bahwa mahasiswa tidak dapat melakukan perubahan data sendiri namun harus terlebih dahulu lewat admin dan prosedur yang ada.
4. Apa saja ancaman yang pernah terjadi terhadap data dan aset yang kritikal dan sensitif yang disebutkan diatas?	Sebelum ada kebijakan mahasiswa tidak dapat melakukan perubahan data ada beberapa permasahalan seperti data mahasiswa dengan data kelulusan tidak sesuai namun kini telah ada kebijakannya. Selain itu, permasalahan yang lainnya terkadang nilai yang diinputkan dapat berubah namun kasusnya tidak banyak, hanya saja hal tersebut mengganggu, karena tentunya kepercayaan akan data nilai yang lainnya akan diragukan, apakah nilai yang lain telah benar seperti itu.
5. Apakah STIE Perbanas telah memiliki prosedur pengelolaan hak akses?	Sudah ada dengan masing masing harus login terlebih dahulu namun belum terdokumentasi
6. Bagaimana cara STIE Perbanas	Sebenarnya belum ada prosedur khusus untuk pengelolaan hak aksesnya sendiri

Pertanyaan Identifikasi	Jawaban Narasumber
mengelola prosedur hak akses tersebut?	
7. Adakah perbedaan hak akses bagi setiap pemilik hak akses?	Sudah ada, dengan permintaan login ke setiap sistem informasi akademik
8. Bagaimana cara pengelolaan perbedaan hak akses tersebut?	Pada login tersebut ada batasan batasan seperti jika mahasiswa hanya dapat melihat data tidak bisa mengubah data, sedangkan dosen dengan login dapat menginputkan data namun hanya pada batas waktu yang ditentukan, dan apabila melewati batas waktu input datanya harus sepengetahuan bidang akademik dengan pengajuan permintaan dan lewat prosedur terlebih dahulu seperti itu
9. Apakah STIE Perbanas telah memiliki prosedur bagi setiap pemilik hak akses dalam melakukan modifikasi atau pembaharuan data?	Belum ada prosedur khusus mengenai modifikasi atau pembaharuan data, hanya saja ada sebuah prosedur yaitu audit trail yang tujuannya untuk melakukan pelacakan data apabila ada ketidaksesuaian data antara proses di sisfor (sistem informasi akademik dan lainnya) dengan proses manual
10. Seperti apa kontrol akses untuk modifikasi data yang sudah berjalan selama ini?	Hal ini mungkin langsung dapat ditanyakan pada bagian TIK

Pertanyaan Identifikasi	Jawaban Narasumber
11. Apa saja cara yang telah ditempuh dalam mengelola proses modifikasi ataupun pembaharuan data? (seperti : selama proses input data ada kontrol akses yang membatasi, selama pemrosesan data bagaimana?)	Dengan pembatasan pembatasan seperti tadi, sehingga dosen hanya dapat menginputkan nilai pada waktu antara setelah UTS yaitu batas waktunya 3 minggu dan setelah UAS batas waktunya 2 minggu dan jika akan melakukan perubahan nilai harus melalui pengajuan langsung ke bagian akademik
12. Kebutuhan keamanan seperti apa saja yang telah diimplementasikan untuk memastikan modifikasi dan pembaharuan data tetap dapat terjaga akurasi dan kebenarannya?	Yang paling penting bagi bidang akademik yaitu mengenai batasan atau limitasi untuk modifikasi datanya agar data tetap konsisten sehingga tidak muncul masalah ketidaksesuaian data
13. Apakah STIE Perbanas telah memiliki prosedur dalam pencegahan (*preventing*) terhadap	Sebenarnya belum ada prosedur khusus yang terdokumentasi mengenai bagaimana sebaiknya pengelolaan pada software maupun hardware seperti server seperti itut, namun pada ruangan server sendiri kondisinya sudah ada penataan kabel, sudah ada detektor asap

Pertanyaan Identifikasi	Jawaban Narasumber
kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	dan hal hal lain yang pada umumnya ada untuk pengamanan
14. Langkah pencegahan (*preventing*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan informasi setiap saat?	Selain menjaga lokasi server, sudah dilakukan sebenarnya proses seperti *backup* data dan proses *restore* data yang dilakukan secara berkala namun untuk teknisnya bagian TIK yang lebih mengetahui
15. Apakah STIE Perbanas telah memiliki prosedur dalam pemulihan (*recovery*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Untuk *recovery* sendiri sudah ada proses *restore* seperti saat terjadi kebakaran beberapa minggu yang lalu, sebenarnya data akademik berhasil di restore dalam waktu kurang lebih 3 hari namun ada pula kehilangan data khususnya pada data diktat ajar dosen karena tidak berhasil *restore* pada data yang ada di e-learning
16. Langkah	Khusus untuk server sudah ada

Pertanyaan Identifikasi	Jawaban Narasumber
pemulihan (*recovery*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan informasi setiap saat?	penangkal petir, kemudian peletakan lokasi server sudah mengikuti pengamanan pada umumnya dengan adanya pemantauan suhu ruangan, detektor dan lainnya dan sarana gedung sudah mulai diperbaiki

C. Identifikasi Ancaman Serta Kebutuhan Keamanan

Tabel A. 2 Hasil wawancara identifikasi ancaman serta kebutuhan keamanan

Pertanyaan Identifikasi	Jawaban Narasumber
1. **Seberapa sering masing masing ancaman (yang disebutkan sebelumnya) tersebut terjadi?**	Untuk nilai akademik yang berubah sebenarnya setiap semester terjadi hanya kasusnya tidak banyak, namun hal tersebut sangat mengganggu karena mengakibatkan nilai lainnya tidak dapat dipastikan kebenarannya sehingga perlu dilakukan pengecekan dan memakan waktu
2. **Apakah dampak dari masing masing ancaman (yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?**	Dampaknya mungkin tidak secara langsung mengganggu proses bisnis hanya saja seperti permasalahan perubahan nilai akademik tersebut akan mengakibatkan data lain menjadi tidak dapat dipercaya namun secara keseluruhan tidak pernah ada dampak sampai kehilangan data
3. **Apakah telah ada**	Secara dokumentasi belum ada

Pertanyaan Identifikasi	Jawaban Narasumber
prosedur keamanan yang diterapkan untuk mengatasi dampak ancaman (yang disebutkan sebelumnya) tersebut? Seperti apa?	namun sebenarnya sudah dilakukan praktek pengamanannya seperti tadi batasan perubahan nilai oleh dosen, batasan mahasiswa tidak dapat merubah data kemudian ada proses backup dan proses restore namun
4. **Kebutuhan keamanan seperti apa yang dibutuhkan berdasarkan masing masing ancaman (yang disebutkan sebelumnya)?**	Mungkin jika kebutuhan keamanan secara teknis bagian TIK yang akan lebih memahami namun dari sudut pandang saya mungkin dibutuhkan standard untuk keamanannya dan kini memang Perbanas sedang mengembangkan blue print TIK untuk memastikan pengelolaan TIK nya

LAMPIRAN B : HASIL WAWANCARA DENGAN KASIE TIK STIE PERBANAS

II. Informasi Interview 2

- Nama Narasumber : Hariadi Yutanto, S.Kom, M.Kom
- Jabatan : Kasie TIK (Manajemen Jaringan dan Technical Support)
- Jenis Kelamin : L
- Tanggal & Waktu : 22 Oktober 2015

A. Informasi Narasumber

1. Apakah peran dan tanggung jawab anda sebagai Kasie TIK?

   Mengelola perangkat keras, perangkat lunak, dan jaringan secara terintegrasi, sebagai *system administrator,* melakukan instalasi perangkat keras computer dan jaringan di seluruh unit kerja, sebagai *network administrator,* mengelola database server, mengendalikan dan mengkoordinasikan tugas *technical support* terhadap *hardware* dan perangkat lunak *operating system*.

2. Apa sajakah aktivitas utama dalam bagian TIK di STIE Perbanas?

   Mengelola layanan TI untuk mahasiswa dan staff yang terdiri dari Simas (sistem informasi akademik mahasiswa) dan sistem informasi staf, e-learning yang berisi materi perkuliahan, e-mail, hotspot, dan login file server, dan selain itu mengelola seluruh aset TIK (hardware, software, dan jaringan). Dan layanan TI yang khusus diberikan untuk mahasiswa adalah email, hotspot dan file server.

3. Bagaimana proses umum penerapan TI pada Bagian TIK di STIE Perbanas?

   Proses yang berjalan diawali dengan pendaftaran mahasiswa baru dengan menggunakan sistem SPMB online. Kemudian data mahasiswa tersebut akan disimpan di bagian kemahasiswaan. Lalu, terdapat sistem SIMAS

yang terdiri dari sistem informasi akademik, kemahasiswaan, keuangan, dan dosen dapat melakukan proses KRS, memasukan nilai (untuk dosen) dan melihat nilai (untuk mahasiswa), dan berbagai aktivitas akademik lainnya. Kemudian, dalam sistem e-learning mahasiswa dapat mengambil materi perkuliahan dan memudahkan dosen untuk proses mengajar. Selain itu, terdapat juga sistem perpustakaan untuk dapat mengakses penelitian dan tugas akhir mahasiswa.

B. Pertanyaan mengenai Keamanan Akses Informasi terkait Kendali Akses

Tabel B. 1 Hasil wawancara keamanan aset informasi terkait kendali akses

Pertanyaan Identifikasi	Jawaban Narasumber
1. Menurut anda, apa sajakah data dan aset yang kritikal dan sensitive dalam operasional di STIE Perbanas?	Seluruh data yang ada di Sistem informasi seperti Simas dan sistem informasi staf serta seluruh data yang ada pada file server karena data ini untuk masing masing unit kerja dan data yang ada di elearning karena isinya tentang materi ajar dosen. Aset yang kritis tentu saja server, PC, jaringan.
2. Siapa saja yang memiliki hak akses terhadap data dan aset yang kritikal dan sensitive yang disebutkan diatas?	Setiap civitas memiliki hak akses terhadap data tersebut, namun dibatasi dari sistem loginnya. Sehingga data yang dapat diakses disesuaikan dengan *role* nya masing masing. Untuk hak akses terhadap server hanya admin dan staff yang bertugas menjaga ruang server saja yang boleh masuk.
3. Dimana saja data dan aset yang kritikal dan	Untuk server kritis yaitu server untuk SIMAS, kepegawaian dan perpustakaan disimpan dalam ruangan

Pertanyaan Identifikasi	Jawaban Narasumber
sensitive yang disebutkan diatas disimpan?	satu ruangan server sendiri. Dan untuk database nya menggunakan postgree. Dan servernya vmware. Untuk server ditempatkan di gedung 1.
4. Apa saja praktek pengamanan yang telah dilakukan oleh STIE Perbanas terhadap data dan aset yang kritikal dan sensitive yang disebutkan diatas?	Usaha yang telah dilakukan oleh organisasi untuk pengamanan antara lain memasang firewall untuk keamanan sistem.. Khusus untuk akses langsung pada database yaitu untuk melakukan mengakses langsung dan modifikasi database hanya dapat dilakukan oleh satu orang administrator. Lalu, juga telah dilakukan back up data penting setiap harinya di waktu tertentu. Dan juga organisasi telah berusaha melakukan sosialisasi keamanan kepada mahasiswa. Untuk server sudah menerapkan aturan standar pengamanan, dan untuk jaringan kami sudah memasang anti netcut juga.
5. Apa saja ancaman yang pernah terjadi terhadap data dan aset yang kritikal dan sensitif yang disebutkan diatas?	Kerusakan pada server dan juga hardware dapat menjadi ancaman terhadap hilangnya data. Selain itu, pernah terjadi kasus mahasiswa mencoba mengambil soal melalui sebuah aplikasi, kasus tersebut terjadi satu kali. Kemudian ancaman lain yang tidak luput seperti virus, adanya *breach* tentu saja, adanya data *saved password* yang dicuri.
6. Apa saja kebutuhan pengamanan untuk masing	Tentu saja memasang firewall dan antivirus untuk keamanan sistem. Juga diperlukan penerapan beberapa peraturan untuk menjaga keamanan

Pertanyaan Identifikasi	Jawaban Narasumber
masing data dana set yang kritikal dan sensitive yang disebutkan diatas?	dari aset TI. Selain itu, juga sudah dibuatkan sebuah *file directory*. Dan Karena pada umumnya selain permasalahan pada sistem, hardware maupun software, terkadang kurangnya *awareness* dari individu masing masing juga menjadi permasalahan dalam keamanan informasi. Kebutuhan pengamanannya tergantung masing-masing aset, yang pada intinya bisa tetap menunjang proses bisnis ketika terjadi suatu kendala.
7. Apakah STIE Perbanas telah memiliki prosedur pengelolaan hak akses?	Sebenernya telah ada prosedurnya, namun tidak terdokumentasikan. Prosedur yang sudah berjalan yaitu pada sistem login dimana terdapat sistem login untuk civitas pada wifi, file server dan seluruh sistem informasi yang disebutkan tadi.
8. Bagaimana cara STIE Perbanas mengelola prosedur hak akses tersebut?	Pengelolaannya lewat login, yaitu pada 1 file server yang digunakan untuk banyak unit kerja, maka aksesnya dibedakan dan dilakukan juga berulang kali *update roles* dikarenakan proses perputaran pegawai dalam unit kerja terus berubah setiap beberapa waktu, dan hal ini berlum terdapat prosedurnya.
9. Adakah perbedaan hak akses bagi setiap pemilik hak akses?	Iya sudah ada, sistem login sudah berjalan dan dalam blue print TIK yang akan dikembangkan akan dilakukan diimplementasikan SSO (*Singel Sign On*) namun masih

Pertanyaan Identifikasi	Jawaban Narasumber
	berusaha ditinjau oleh manajemen atas.
10. Bagaimana cara pengelolaan perbedaan hak akses tersebut?	Pertama adanya portal login lewat WPA/WP, kemudian mahasiswa tida dapat akses lokal atau mengakses jaringan dosen, mahasiswa hanya akses langsung ke internet, kemudian file server mahasiswa dan dosen berbeda dari loginnya dan akses wifi juga melalui login serta melakukan terus menerus *update roles* untuk akses pengguna.
11. Apakah STIE Perbanas telah memiliki prosedur dalam pencegahan (*preventing*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Ada beberapa prosedur yang telah ada namun ada yang telah dijalankan dan ada juga yang belum. Contoh SOP yang telah dijalankan adalah mengenai SLA, jaringan LAN, Maintenance, jaringan Internet dan pembuatan Email. Salah satu SOP yang belum dijalankan adalah SOP mengenai pengelolaan komplain. Selain itu SOP mengenai penanganan bencana belum ada.
12. Langkah pencegahan (*preventing*) seperti apa yang sudah dilakukan untuk menjaga ketersediaan informasi setiap	Organisasi melakukan backup pada database setiap hari, biasanya pada malam hari. Selain itu juga dilakukan backup server dan NAS (Network-Attached Storage). Penataan kabel sudah ada. Masing – masing kabel sudah ditata sendiri-sendiri dan masing masing kabel telah memiliki label

Pertanyaan Identifikasi	Jawaban Narasumber
saat?	untuk mempermudah pengaturan.
13. Apakah STIE Perbanas telah memiliki prosedur dalam pemulihan (*recovery*) terhadap kerusakan hardware maupun software yang mengakibatkan tempat penyimpanan data tersebut terancam?	Prosedur dalam bentuk SOP mungkin tidak tapi sebenarnya sudah dilakukan back up data setiap malam. Dan untuk recovery juga belum ada namun saat kemaren terjadi kebakaran recovery data dan restore data berhasil dilakukan hanya saja ada beberapa data yang tidak dapat terselematkan yaitu data e learning, untuk data simas sendiri berhasil diselamatkan seluruhnya.
14. Berapa kali organisasi melakukan *maintenance* terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi?	Pada awal semester (6 bulan sekali) organisasi melakukan maintenance keseluruhan untuk setiap kelas dan lab yang kemudian akan menghasilkan laporan. Apabila ada kerusakan maka akan diserahkan kebagian Umum yang kemudian bertugas memanggil orang untuk memperbaiki atau mengganti aset. Selain itu maintenance untuk lab juga dilakukan sebelum aktivitas UAS dan UTS dan juga nantinya akan menghasilkan laporan.

C. Identifikasi Ancaman serta Kebutuhan Keamanan

Tabel B. 2 Hasil wawancara terkait ancaman dan kebutuhan keamanan

Pertanyaan Identifikasi	Jawaban Narasumber
1. **Seberapa sering**	Untuk data KRS yang dirubah dan

Pertanyaan Identifikasi	Jawaban Narasumber
masing masing ancaman (yang disebutkan sebelumnya) tersebut terjadi?	dihapus karena menyebarkan password hampir terjadi setiap KRS berlangsung hanya saja kasusnya tidak banyak. Selain itu ancaman lainnya terjadi namun dengan kasus yang tidak banyak.
2. **Apakah dampak dari masing masing ancaman (yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?**	Dampak dari ancaman KRS sebenarnya mengakibatkan proses KRS terganggu namun tidak besar dampaknya. Namun dampak yang paling terasa adalah kebakaran kemaren, mungkin karena tidak adanya prosedur yang benar sehingga terjadi kebakaran tersebut.
3. **Apakah telah ada prosedur keamanan yang diterapkan untuk mengatasi dampak ancaman (yang disebutkan sebelumnya) tersebut? Seperti apa?**	Organisasi belum menerapkan standard keamanan tertentu hanya ada beberapa prosedur yang dibuat mengenai pengelolaan SI/TI.
4. **Kebutuhan keamanan seperti apa yang dibutuhkan berdasarkan masing masing ancaman (yang disebutkan sebelumnya)?**	Organisasi telah memasang firewall dan antivirus untuk keamanan sistem. Selain itu untuk keamanan Wifi juga telah dipasang *anti-netcut*. Organisasi juga telah menerapkan beberapa peraturan untuk menjaga keamanan dari aset TI. Selain itu organisasi juga berencana akan membuat DRP untuk keamanan saat terjadi bencana. Selain itu, karena kelemahan teknis yang

Pertanyaan Identifikasi	Jawaban Narasumber
	dimiliki oleh organisasi antara lain adalah firewall yang digunakan hanya microtix, belum ada mirroring untuk database selain itu mahasiswa juga belum bisa reset password sendiri harus manual melalui admin TI, maka akan dibutuhkan sistem SSO tadi.

(Halaman ini sengaja dikosongkan)

LAMPIRAN C : HASIL PENILAIAN RISIKO (*RISK REGISTER*)

Tabel C. 1Hasil Penilaian Risiko

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
Hardware	Kerusakan pada Server	Proses bisnis terhambat	8	Seluruh sistem seperti SIMAS, kepegawaian dan perpustakaan berada pada 1 fisik server sehingga apabila server mengalami kerusakan dampaknya akan menghambat proses bisnis hingga penurunan	Gempa bumi	3	Kemungkinan terjadi kecil	Letak lokasi ruang server di lantai 2	5	Kontrol yang dilakukan sudah mampu mengamankan aset server namun keefektifannya masih rata-rata	**120**	High	Bagian Umum
					Badai dan Petir	5	Kemungkinan terjadi 2 kali setahun	Terdapat penangkal petir	2	Kontrol yang dilakukan sudah mampu mengamankan aset server dari risiko kerusakan	**80**	Medium	Bagian Umum
					Banjir	5	Kemungkinan terjadi 2 kali setahun	Letak lokasi ruang server di	2	Kontrol yang dilakukan sangat efektif untuk	**80**	Medium	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				citra organisasi. Selain itu, secara finansial kerusakan server membutuhkan biaya pengadaan yang tinggi				lantai 2		menanggulangi kemungkinan terjadinya risiko kerusakan akibat banjir			
		Penurunan citra organisasi			Kebakaran	2	Terjadi tahun lalu namun kecil sekali kemungkinannya	Terdapat smoke detector dan *fire extinguisher*	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan akibat kebakaran berulang	**48**	Low	Bagian Umum
		Organisasi mengalami kerugian secara finansial			Kebocoran dan Kerusakan pada Bangunan	5	Kemungkinan terjadi 2 kali setahun	Terdapat maintenance yang dilakukan 6 bulan sekali	5	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan	**200**	Very High	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
										berkala setiap 3 bulan			
	Server berhenti	Proses bisnis terhambat	7	Terhambatnya proses bisnis akibat server berhenti bekerja dapat mengakibatkan ketidakpuasan dari seluruh civitas karena seluruh sistem yang digunakan berada pada satu server fisik	Kerusakan pada Genset dan UPS	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah memiliki UPS dan Genset	Lokasi genset dan UPS terdapat pada lokasi aman dan terdapat maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko dengan adanya UPS dan Genset	**56**	Medium	Bagian TIK
					Listrik Mati	7	Kemungkinan terjadinya tinggi tiap bulannya	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko dengan adanya UPS dan Genset	**98**	Medium	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Kinerja server menurun	Berkurangnya kepercayaan civitas akademika	3	Kinerja server menurun dapat mengakibatkan berkurangnya kepercayaan dari civitas karena seluruh sistem berada pada satu sistem namun menurunnya kinerja server hanya berdampak kecil pada berjalannya keseluruhan proses bisnis	RAM mengalami kelebihan memori	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**48**	Low	Bagian TIK
		Menurunnya prouktivitas			Kinerja Procesor menurun akibat terlalu banyak kapasitas data	3	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**36**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
					Tempat penyimpanan (*Harddisk)* penuh	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Maintenance dilakukan 6 bulan sekali	4	Kontrol yang dilakukan sudah cukup namun secara best practice seharusnya maintenance dilakukan berkala setiap 3 bulan	**48**	Low	Bagian TIK
	Pencurian data	Penurunan citra organisasi	5	Pencurian data dapat mengakibatkan tersebarnya data dan bocornya data penting akademik dan hal ini dapat mengakibatkan penurunan	Ruang Server kurang diberi pengamanan	5	Kemungkinan terjadinya bisa paling tidak 2 kali setahun karena belum memiliki standard prosedur pengamanan ruang server	Ruang server dikunci dan tidak semua dapat masuk ke dalam ruangan	4	Kontrol yang dilakukan sudah cukup namun belum ada log book mengenai siapa saja yang masuk kedalam ruang server	**100**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Penyalahgunaan data		citra organisasi namun pencurian data tidak mengakibatkan hilangnya data dan dampak yang diakibatkan cukup tinggi	Kesalahan Konfigurasi Server	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena telah dilakukan maintenance berkala setiap 6 bulan	Terdapat pelatihan terhadap staf bagian TIK	5	Kontrol yang dilakukan sudah sesuai namun sosialisasi yang dilakukan kurang memberikan pengaruh terhadap awareness civitas atas keamanan data	**100**	Medium	Bagian TIK
	Data Hilang	Proses bisnis terhambat	7	Data hilang dapat menghambat berjalannya proses bisnis ketika data mengenai kemahasiswaan dan	Kesalahan DBA	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena DBA telah terlatih	Melakukan pelatihan pada DBA	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko *human eror* pada DBA	**84**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				akademik dibutuhkan sehingga dampaknya cukup tinggi	Virus	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena dilakukan maintenance dan pengecekan lisensi oleh bagian TIK	Memasang antivirus E-scan	4	Kontrol yang dilakukan sudah cukup baik dan bagian TIK telah melakukan pengecekan setiap 6 bulan sekali	**112**	Medium	Bagian TIK
	Kerusakan pada PC	Menurunnya produktivitas	4	Kerusakan PC dapat menghambat aktivitas dalam proses bisnis yang didukung	Gempa Bumi	3	Kemungkinan terjadi kecil	Letak lokasi ruang kerja di lantai 2	5	Kontrol yang dilakukan sudah mampu mengamankan PC namun keefektifannya masih rata-rata	**60**	Low	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Organisasi mengalami kerugian secara finansial		oleh TI dan hali ini mengakibatkan menurunnya kinerja dan terhambatnya proses bisnis serta mengakibatkan kerugian secara finansial bagi organisasi namun dampak yang diakibatkan tidak begitu tinggi karena proses utama perkuliahan tetap dapat berjalan	Badai dan Petir	5	Kemungkinan terjadi bisa 2 kali setahun	Terdapat penangkal petir	2	Kontrol yang dilakukan sudah mampu mengamankan PC dari risiko kerusakan	**40**	Low	Bagian Umum
					Banjir	5	Kemungkinan terjadi bisa 2 kali setahun	Letak lokasi ruang server di lantai 2	2	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan PC akibat banjir	**40**	Low	Bagian Umum
		Proses bisnis terhambat			Kebakaran	2	Terjadi tahun lalu namun kecil sekali kemungkinannya	Terdapat smoke detector dan *fire extinguisher*	3	Kontrol yang dilakukan sangat efektif untuk menanggulangi kemungkinan terjadinya risiko kerusakan PC akibat	**24**	Low	Bagian Umum

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
										kebakaran berulang			
					Kebocoran dan Kerusakan pada Bangunan	5	Kemungkinan terjadi bisa 2 kali setahun	Terdapat maintenance yang dilakukan 6 bulan sekali	4	Kontrol yang dilakuka cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**80**	Medium	Bagian Umum
					Keyboard, mouse atau monitor mengalami kerusakan karena pemakaian berlebih	3	Kemungkinan terjadinya kecil	Terdapat maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sudah cukup baik dan bagian TIK telah melakukan pengecekan prasarana secara berkala	**24**	Low	Bagian TIK
	PC tidak dapat menyala	Menurunnya produktivit	3	Dampak yang diakibatkan tidak terlalu	Kerusakan pada Genset dan	4	Kemungkinan terjadi setiap tahunnya	Terdapat maintenance yang	4	Kontrol yang dilakukan cukup baik	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		as		tinggi karena hanya menghambat aktivitas yang membutuhkan dukungan TI namun secara keseluruhan proses perkuliahan tetap dapat berjalan dengan baik	UPS		namun kecil sekali karena kontrol yang telah dilakukan	dilakukan 6 bulan sekali		namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali			
					Listrik Mati	7	Kemungkinnan terjadinya sangat tinggi	Sudah terdapat genset saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**42**	Low	
	PC terkena virus	Menurunnya produktivitas	3	Dampak yang diakibatkan tidak terlalu tinggi karena hanya menghambat aktivitas yang membutuhkan dukungan TI namun secara keseluruhan	antivirus tidak update	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Terdapat antivirus e-scan	5	Kontrol yang dilakukan cukup yaitu dengan menggunakan antivirus E-Scan	**60**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				proses perkuliahan tetap dapat berjalan dengan baik									
Software	Aplikasi tidak dapat diakses	Proses bisnis terhambat	5	Proses bisnis akan terhambat akibat aplikasi tersebut menjadi pendukung dalam proses perkuliahan seperti e-learning dimana seluruh materi ajar dosen berada	Listrik Mati	7	Kemungkinnan terjadinya sangat tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian Umum
		Menurunnya produktivitas			Server Down	5	Kemungkinan terjadi bisa 2 kali setahun	Adanya perawatan maintenance pada server 6 bulan sekali	3	Kontrol yang dilakukan sudah cukup baik untuk menanggulangi permasalahan server	**75**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				pada sistem tersebut									
	Aplikasi diakses oleh pihak yang tidak berwenang	Tersebarluasnya data orgnisasi	8	Dengan diaksesnya aplikasi oleh pihak yang tidak berwenang dapat mengakibatkan bocornya data akademik dan kemahasiswaan serta data lain yang sifatnya *confidential* sehingga dapat yang diakibatkan sangat tinggi	Kesalahan dalam pemberian hak akses	4	Kemungkinan terjadinya sekali setahun	Adanya peraturan dalam pembatasan hak akses	4	Kontrol yang dilakukan sudah cukup baik namun masih kurang mampu faktor eksternal yang berusaha masuk kedalam sistem	**128**	High	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
Data	Data tidak dapat diakses	Menurunnya produktivitas	5	Data tidak dapat diakses mengakibatkan penurunan kinerja dan terhambatnya proses bisnis hanya pada aktivitas yang membutuhkan dukungan TI sehingga dampak yang dihasilkan tidak menyeluruh dan tinggi	Listrik Mati	7	Kemungkinan terjadinya tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian TIK
		Proses bisnis terhambat			Server Down	5	Kemungkinan terjadi bisa 2 kali setahun	Adanya perawatan maintenance pada server 6 bulan sekali	3	Kontrol yang dilakukan sudah cukup baik untuk menanggulangi permasalahan server	**75**	Low	Bagian TIK
		Berkurangnya kepercayaan civitas akademika											Bagian TIK
	Pencurian data	Berkurangnya kepercayaan civitas akademika	7	Pencurian data dapat mengakibatkan tersebarnya data dan bocornya data penting	Terdapat hacker yang mencuri data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah	Adanya firewall dan pengamanan jaringan	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	**140**	High	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				akademik dan hal ini dapat mengakibatkan berkurangnya kepercayaan civitas dan dampak yang diakibatkan cukup tinggi			dilakukan						
	Manipulasi data	Komplain dari civitas akademika	8	Manipulasi data akademik dan mahasiswa dapat mengakibatkan komplain dan	Username dan password diketahui oleh pengguna lain	5	Kemungkinan terjadi bisa 2 kali setahun	Diadakan sosialisasi kepada civitas akademika	5	Kontrol yang dilakukan sudah cukup untuk meningkatkan awareness civitas terhadap data *confidential*	**200**	Very High	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
		Berkurangnya kepercayaan civitas akademika		berkurangnya kepercayaan civitas terhadap pengamanan yang sudah dilakukan oleh organisasi sehingga hal ini berdampak cukup tinggi karena beberapa data bersifat *confidential*	Terdapat hacker yang memanipulasi data	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Adanya firewall dan sosialisasi dari Bagian TIK ke civitas	5	Kontrol yang dilakuan sudah cukup untuk mengamankan data dari hacker	**160**	High	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Backup data gagal	Informasi yang ditampilkan tidak terbaru/terkini	4	Backup data gagal tidak berdampak cukup besar terhadap proses bisnis karena telah ada kontrol notifikasi dari sistem apabila back up data mengalami kegagalan, sehingga pihak TIK telah dapat mengatasi dampaknya dengan cepat	Kapasitas media penyimpanan overload	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Maintenance oleh DBA	3	Kontrol yang dilakukan sudah cukup baik dengan maintenance yang dilakukan sehingga kapasitas penyimpanan selalu terkontrol	**48**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Data hilang	Komplain dari civitas akademika	8	Data hilang dapat menghambat berjalannya proses bisnis ketika data mengenai kemahasiswaan dan akademik dibutuhkan sehingga dampaknya cukup tinggi	Server Rusak	3	Kemungkinan terjadinya kecil	Melakukan maintenance yang dilakukan 6 bulan sekali serta backup data setiap harinya	4	Kontrol yang dilakukan sudah cukup naik namun berdasarkan *best practice* seharusnya dilakukan selama 3 bulan sekali	**96**	Medium	Bagian TIK
		Proses bisnis terhambat			Virus/Bug	5	Kemungkinan terjadi bisa 2 kali setahun	Adanya antvirus e-scan	4	Kontrol yang dilakukan sudah cukup baik dan sesuai untuk menanggulangi virus	**160**	High	Bagian TIK
Jaringan	Kurangnya kontrol pengamanan kabel	Proses bisnis terhambat	5	Kabel merupakan komponen yang penting untuk	Kabel rusak	5	Kemungkinan terjadi bisa 2 kali setahun karena adanya hewan	Sudah ada pelabelan dan pengatura	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan	**50**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				memastikan hubungan antar perangkat keras sehingga dampak yang diakibatkan cukup tinggi			pengerat	n kabel		kabel terkelola dengan baik			
	Internet Mati	Produktivitas menurun	5	Internet mati dapat mengakibatkan terhambatnya aktivitas yang membutuhkan dukungan TI dan cukup berdampak pada keseluruhan aktivitas dalam proses bisnis	Listrik Mati	7	Kemungkinan terjadinya tinggi	Sudah terdapat genset dan UPS saat listrik mati	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi listrik mati	**70**	Low	Bagian Umum
					Wifi rusak	3	Kemungkinan terjadinya kecil karena adanya kontrol yang telah dilakukan	Melakukan maintenance yang dilakukan 6 bulan sekali	2	Kontrol yang dilakukan sudah sangat baik untuk mengatasi kerusakan wifi	**30**		Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
					Genset mati	4	Kemungkinan terjadi setiap tahunnya namun kecil sekali karena kontrol yang telah dilakukan	Melakukan maintenance yang dilakukan 6 bulan sekali	4	Kontrol yang dilakukan cukup baik namun secara best practice seharusnya maintenance dilakukan 3 bulan sekali	**80**	Medium	Bagian TIK
					Kabel Rusak	5	Kemungkinan terjadi bisa 2 kali setahun karena adanya hewan pengerat	Sudah ada pelabelan dan pengaturan kabel	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan kabel terkelola dengan baik	**50**	Low	Bagian TIK
	Akses internet lambat	Komplain dari civitas akademika	5	Akses internet lambat dapat mengakibatkan banyaknya komplain dan	Kesalahan Konfigurasi	5	Kemungkinan terjadi bisa 2 kali setahun	Melakukan maintenance 6 bulan sekali	4	Kontrol yang dilakukan cukup baik namun secara best practice seharusnya	**100**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				menurunnya produktivitas karena pada umumnya banyak aktivitas yang didukung oleh TI sehingga dampak yang dihasilkan cukup tinggi						maintenance dilakukan 3 bulan sekali			
		Produktivitas menurun			Ada yang melakukan netcut	7	Kemungkinan terjadinya tinggi	Memasang anti netcut	2	Kontrol yang dilakukan saat ini sudah sangat baik untuk memastikan tidak ada lagi yang dapat melakukan netcut	**70**	Low	Bagian TIK
Sumber Daya Manusia	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat berdampak	Penurunan Kompetensi Karyawan Pegawai Non-TI	3	Kemungkinan terjadinya kecil karena adanya kebijakan dan etika kerja untuk pegawai	Adanya pelatihan untuk Pegawai Non-TI	4	Kontrol yang dilakukan cukup baik untuk mengatasi adanya penyalahgunaan data dalam internal organisasi	**60**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Adanya praktik KKN di perusahaan	2	Kemungkinan terjadinya sangat kecil karena adanya kebijakan dan etika kerja untuk pegawai	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**30**	Low	Pengguna SISFO
	Data yang ada tidak valid	Penurunan citra organisasi Komplain dari civitas akademika	5	Data yang ada tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah pada pemrosesan dan output data sehingga hasil yang ditampilkan	Kesalahan dalam input data	5	Kemungkinan terjadi bisa 2 kali setahun seperti kesalahan mengetik atau memasukan data pada sistem seperti sistem kepegawaian dan keuangan	Adanya pelatihan untuk karyawan	3	Kontrol yang dilakukan sudah baik untuk mengatasi kesalahan berulang dilakukan oleh pegawai	**75**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				akan berbeda dan hal ini mengakibatkan ketidakpuasan civitas hingga penurunan citra organisasi									
	Pelanggaran regulasi hak akses	Berkurangnya kepercayaan civitas akademika	3	Pelanggaran regulasi hanya mungkin terjadi pada internal organisasi dimana pada umumnya terjadi di lingkungan pegawai	Penyalahgunaan akses regulasi	3	Kemungkinan terjadinya kecil karena namun regulasi terjadi hampir setiap 2 tahun dan pelanggaran akses mungkin terjadi baik yang diketahui maupun tidak	Adanya kebijakan dan prosedur regulasi	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya penyalahgunaan akses oleh pegawai	**27**	Low	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat berdampak besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Penurunan Kompetensi Pegawai TI	3	Kemungkinan terjadinya kecil	Adanya pelatihan untuk Pegawai TI	4	Kontrol yang dilakukan cukup baik untuk mengatasi adanya penyalahgunaan data dalam internal organisasi	**60**	Low	Penggguna SISFO
					Adanya praktik KKN di perusahaan	3	Kemungkinan terjadinya kecil karena telah ada kebijakan dan aturan etika kerja pegawai	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**45**	Low	Penggguna SISFO
	Data yang ada tidak valid	Komplain dari civitas akademika	6	Data yang ada pada database dan dikelola oleh pegawai TI apabila	Kesalahan dalam input data	6	Kemungkinan terjadinya cukup tinggi karena pegawai TI	Adanya pelatihan untuk karyawan	3	Kontrol yang dilakukan sudah baik untuk mengatasi kesalahan	**108**	Medium	Bagian TIK

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah mengakibatkan menurunya kepercayaan civitas hingga mengakibatkan menurunnya kepuasan dari civitas dan dapat mengakibatkan pula menurunnya reputasi			selalu berhubungan dengan sistem			berulang dilakukan oleh pegawai			

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Pelanggaran regulasi	Penurunan citra organisasi	3	Pelanggaran regulasi hanya mungkin terjadi pada internal organisasi dimana pada umumnya terjadi di lingkungan pegawai	penyelahgunaan akses regulasi	4	Kemungkinan terjadinya rendah, paling banyak sekali setahun	Adanya kebijakan dan prosedur regulasi	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya penyalahgunaan akses oleh pegawai	**36**	low	Penggun a SISFO
	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Tersebarluasnya data organisasi mengakibatkan hilangnya kerahasiaan dari data dan hal ini sangat	Penurunan Kompetensi Dosen	3	Kemungkinan terjadinya kecil	Adanya kebijakan dan etika kerja	4	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelanggaran etika kerja oleh pegawai	**60**	Low	Penggun a SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
				berdampak besar karena dapat mengakibatkan pula hilangnya kepercayaan civitas	Adanya praktik KKN di perusahaan	2	Kemungkinan terjadinya sangat kecil	Adanya kebijakan dan etika kerja	3	Kontrol yang dilakukan sudah baik untuk mengatasi adanya pelangaran etika kerja	**30**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Data yang ada tidak valid	Komplain dari civitas akademika	5	Data yang ada tidak valid memiliki nilai cukup tinggi karena dampak yang dihasilkan adalah pada pemrosesan dan output data sehingga hasil yang ditampilkan akan berbeda dan hal ini mengakibatkan ketidakpuasan civitas hingga penurunan citra organisasi	Kesalahan dalam input data nilai	5	Kemungkinan terjadi bisa 2 kali setahun walau kasusnya tidak banyak	Adanya pelatihan untuk dosen	3	Kontrol yang dilakukan sudah baik untuk mengatasi kesalahan berulang dilakukan oleh pegawai	**75**	Low	Pengguna SISFO

Kategori Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Justifikasi Pemberian nilai	Penyebab Potensi Kegagalan	Occ	Justifikasi Pemberian Nilai	Proses Kontrol Saat ini	Det	Justifikasi Pemberian nilai	RPN	Level	Pemilik Risiko
	Sharing Password Mahasiswa/i	Komplain dari civitas akademika Penurunan citra organisasi	7	Penyebaran password oleh mahasiswa memiliki dampak yang besar karena data dalam masing masing akun mahasiswa bersifat rahasia, dan sistem *change password* belum dimiliki dalam sistem kemahasiswaannya dan hanya admin yang dapat mengubah passoword	Manipulasi data	6	Terjadi hampir disetiap FRS semester baru walau dengan kasus yang tidak banyak	Sosialisasi kepada mahasiswa/i	5	Kontrol yang dilakukan kurang dapat mengatasi kurangnya awareness mengenai pentingnya menjaga kerahasiaan data	**210**	Very High	Pengguna SISFO

LAMPIRAN D : JUSTIFIKASI PEMETAAN RISIKO DENGAN KONTROL ISO/IEC:27002:2013

Tabel D. 1Justifikasi pemetaan kebutuhan kontrol pada kerangka kerja ISO/IEC:27002:2013

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO/IEC:27002:2013	Justifikasi
Sumber Daya Manusia	Mahasiswa	26	Manipulasi data	Sharing password mahasiswa/i	*9.1.1 Access control policy*	Kontrol yang memuat aturan/kebijakan dalam menggunakan hak akses di sebuah organisasi. Kontrol ini bertujuan untuk menjamin persyaratan kendali akses terhadap informasi dan fasilitas sistem informasi didefinisikan dengan tepat.

						Kebijakan kendali akses harus ditetapkan, didokumentasikan dan diulas berdasarkan kebutuhan keamanan bisnis dan informasi.
Data	Data demografi mahasiswa, Data akademik dan Data file server	13	Manipulasi data	Username dan password diketahui oleh pengguna lain	*9.2.1 User registration and de-registration*	Kontrol dalam mengendalikan pendaftaran dan penghapusan hak akses terhadap fasilitas sistem informasi dalam organisasi. Kontrol ini bertujuan untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses tidak sah ke dalam sistem maupun layanan informasi.
					9.4.3 Password management system	Kontrol dalam melakukan pengelolaan *password* dan memastikan kualitas dari setiap *password*. Sehingga

						kontrol ini berguna untuk memastikan bahwa penggunaan *password* oleh setiap pengguna telah sesuai dengan standard keamanan
				Terdapat hacker yang memanipulasi data	*9.1.2 Access to networks and network services*	Kontrol dalam memberikan batasan ke dalam jaringan dan juga layanan jaringan. Kontrol ini bertujuan untuk memberikan batasan akses jaringan dan juga layanan jaringan bagi pengguna sistem sesuai dengan hak aksesnya masing-masing.
		12	Pencurian data	Terdapat hacker yang mencuri data	*9.4.2 Secure log-on procedures*	Kontrol dalam melakukan proses akses masuk sistem dengan aman. Kontrol ini bertujuan untuk mencegah akses oleh orang yang tidak berwenang ke dalam sistem

						dan aplikasi serta memberikan rekomendasi pengamanan yang baik terhadap aspek autentikasi saat melakukan log in pada sistem maupun aplikasi.
Software	SIMAS, E-learning, Perpustakaan	10	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	*9.3.1 Use of Secrets Authentication Information*	Kontrol dalam penggunaan informasi rahasia sebagai pengamanan autentikasi pengguna. Kontrol ini bertujuan untuk membuat pengguna bertanggung jawab untuk menjaga informasi auntentik mereka. Pada kontrol ini pengguna wajib mengikuti praktek-praktek organisasi dalam penggunaan informasi yang sifatnya rahasia.

LAMPIRAN E : REKOMENDASI MITIGASI RISIKO

Tabel E. 1 Rekomendasi Mitigasi Risiko

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
Sumber Daya Manusia	Mahasiswa	26	Manipulasi data	Sharing password mahasiswa/i	*9.1.1 Access control policy*	Untuk menjamin persyaratan kendali akses terhadap informasi dan fasilitas sistem informasi didefinisikan dengan	• Mengandung kebijakan dalam melakukan penyebaran informasi dan otorisasi • Memiliki peraturan yang relevan mengenai pembatasan	• Adanya autentikasi untuk login pengguna SISFO • Adanya perbedaan hak akses untuk masing masing	• Membuat aturan yang jelas mengenai hak akses terhadap aset sistem informasi • Membuat peraturan mengenai pembatasa

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
						tepat.	akses data maupun layanan • Memiliki kebijakan dalam melakukan pendaftaran maupun penghapusan hak akses • Mengandung peraturan mengenai pengelolaan	*role* dalam SISFO • Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI • Sudah dibuat dan dilaksanak	n akses data maupun layanan • Membuat ***kebijakan kendali akses*** yang mengatur mengenai aturan-aturan terkait kendali akses

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013**		
							informasi rahasia • Kebijakan kendali akses harus didukung oleh prosedur terkait manajemen password	an beberapa SOP mengenai SI/TI di organisasi	
Data	Data demografi mahasiswa, Data akademik,	13	Manipulasi data	Username dan password diketahui oleh	*9.2.1 User registration and de-*	Untuk memastikan akses pengguna yang	• Menggunakan *User ID* yang unik untuk menghubungkan pengguna	• Adanya autentikasi untuk login pengguna	• Seluruh perubahan hak akses (penambahan,

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
	dan Data file server			pengguna lain	*registration*	berwenang dan untuk mencegah akses tidak sah ke dalam sistem maupun layanan informasi.	ke dalam aktivitas yang dia lakukan dalam mengakses sistem • Penggunaan *User ID* hanya diizinkan ketika diperlukan untuk kebutuhan bisnis atau	SISFO • Adanya batasan dalam SISFO bahwa perubahan, penambahan dan penghapusan akun dan password pengguna hanya	modifikasi dan penghapusan) harus tercatat dalam sistem dengan baik • Dalam setiap pembuatan *User ID*, masing-masing

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							alasan operasional dan harus didokumentasikan • Segera menonaktifkan atau menghapus *User ID* dari pengguna yang telah meninggalkan organisasi • Melakukan	dapat dilakukan oleh database administrator • Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan	*User ID* harus memiliki *ID* yang unik dan paling tidak memiliki kombinasi huruf dan angka • Melakukan penghapusan *User ID*

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							pengelolaan secara berkala dan menghapus atau menonaktifkan *User ID* yang menggunakan kapasitas secara berlebihan • Memastikan bahwa *User ID* tidak	TI	milik pengguna yang sudah meninggalkan/bebas tugas dari organisasi • Bagian TIK harus mengelola log sistem dengan baik secara berkala

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013**		
							digunakan oleh pihak yang tidak berwenang		• Membuat sebuah ***prosedur user registration dan de-registration***
					9.4.3 Password management system	Untuk mengelola dan memastikan bahwa penggunaan *password*	• Memastikan pemilihan password yang berkualitas • Memastikan sistem tidak	• Adanya batasan dalam SISFO bahwa perubahan, penambah	• SISFO Perbanas membuat aturan penggunaan password

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013**		
						oleh setiap pengguna telah sesuai dengan standard keamanan	menampilkan password dalam kolom password ketika pengguna menginputkannya • Memastikan pengguna mengganti password default pada awal log in • Menyimpan	an dan penghapusan akun dan password pengguna hanya dapat dilakukan oleh database administrator • *Password* yang	yang benar unuk setiap pengguna yang mencakup : - Pengguna diharuskan melakukan request perubahan password apabila informasi

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							data password di database berbeda dari sistem aplikasi data • Menyimpan dan mentransmisikan password dalam cara yang aman (enkripsi) • Menghimbau untuk melakukan	digunakan telah sesuai dengan *strong password*	password diketahui pengguna lain / bocor - Pengguna tidak boleh melakukan *share login* - Mengguna kan aturan *strong password* untuk

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							pergantian password secara berkala sesuai dengan kebutuhan • Mengelola data password dan memastikan tidak ada penggunaan kembali password lama		pengguna seluruh SISFO - Melakukan reset maupun pergantian password pengguna secara berkala sesuai dengan kebijakan yang ada

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
									• Membuat sebuah ***prosedur mengenai manajemen password yang mencakup proses pengelolaan pergantian password***

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013**		
				Terdapat hacker yang memanipulasi data	*9.1.2 Access to networks and network services*	Untuk memberikan batasan akses jaringan dan juga layanan jaringan bagi pengguna sistem sesuai dengan hak aksesnya masing-masing.	• Memuat jaringan dan layanan jaringan apa saja yang boleh diakses • Memiliki prosedur untuk menentukan siapa yang diizinkan untuk mengakses jaringan dan	• Data hanya bisa dimasukkan, diganti atau dihapus oleh *database administrator* saja • Dilakukan *maintenance* Wifi setiap 2	• Membuat daftar jaringan dan layanan jaringan yang boleh diakses oleh public dan yang boleh diakses secara khusus oleh

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							layanan jaringan • Memiliki langkah untuk melindungi akses ke koneksi jaringan dan layanan jaringan • Melakukan monitoring penggunaan layanan jaringan	minggu sekali • Telah dipasang anti netcut untuk keamanan wifi	admin • Memberikan sistem keamanan yang ketat pada jaringan agar tidak mudah dibobol • Membuat sebuah *prosedur mengenai akses*

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	***Control Objective***	**Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013**		
									jaringan
		12	Pencurian data	Terdapat hacker yang mencuri data	*9.4.2 Secure log-on procedures*	Untuk mencegah akses oleh orang yang tidak berwenang ke dalam sistem dan aplikasi serta memberikan rekomendasi pengamanan yang baik terhadap	• Tidak menampilkan sistem atau aplikasi sampai proses log on telah berhasil diselesaikan • Menampilkan pemberitahuan umum yang memperingatkan bahwa	• Data hanya bisa dimasukkan, diganti atau dihapus oleh *database administrator* saja	• Bagian TIK harus mengelola log sistem dengan baik secara berkala • Memberikan sistem pengamanan lebih terhadap data dan

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
						aspek autentikasi saat melakukan log in pada sistem maupun aplikasi.	komputer hanya bisa diakses oleh pengguna yang berwenang • Tidak memberikan bantuan pesan selama prosedur log on yang akan membantu pengguna log in dengan		informasi penting yang ada di database • Melakukan monitoring data dan informasi secara berkala • Bagian TIK harus mengelola

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							cara yang tidak sah • Memvalidasi log on hanya pada penyelesaian semua input data. Jika kondisi kesalahan muncul, sistem tidak harus menunjukkan bagian dari		manajemen user dan password dengan baik • Melakukan update CMS, mengaudit struktur pemrograman secara berkala dan melakukan

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							data mana yang benar atau tidak benar • Melindungi dari upaya brute force log on • Memberikan batasan percobaan terhadap log on yang gagal • Tidak menampilkan		patching pada sistem operasi dan aplikasi • Membuat ***prosedur secure log-on***

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							password yang dimasukkan		
Software	SIMAS, E-learning, Perpustakaan	10	Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	*9.3.1 Use of Secrets Authentication Information*	Untuk membuat pengguna bertanggung jawab untuk menjaga informasi auntentik mereka.	• Memastikan setiap pengguna menjaga kerahasiaan autentikasi informasi • Menghindari penyimpanan password pada lokasi yang bersifat	• Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI • Pada Lab tidak bisa	Bagian TIK membuat aturan / kebijakan penggunaan autentikasi pada akun pengguna yang mencakup : • Pengguna tidak

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							umum (kertas, perangkat lunak, handphone) • Memastikan adanya proteksi terhadap password apabila password digunakan sebagai informasi	menginstall aplikasi dari luar	diperbolehkan melakukan *share* informasi autenttikasi • Pengguna tidak diperbolehkan menyimpan informasi autentikas

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							autentikasi • Apabila password digunakan sebagai autentikasi tidak digunakan untuk kebutuhan bisnis dan kebutuhan non-bisnis • Apabila password		i pada tempat yang dapat dilihat oleh pengguna lain (kertas, *mobile device*) • Ketika password digunakan sebagai

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							digunakan sebagai autentikasi maka password harus memenuhi standard kualitas *strong password* • Tidak membagikan informasi pribadi yang		informasi autentikasi, maka pengguna harus membuat password yang berkualitas Membuat ***kebijakan tanggung jawab pengguna***

Kategori Aset Informasi Kritis	Aset Informasi	ID Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Tindakan mitigasi risiko berdasarkan ISO/IEC:27002:2013			Kontrol yang telah dilakukan (Praktik Keamanan Organisasi)	Rekomendasi Mitigasi Risiko
					Kontrol	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO/IEC:27002:2013		
							bersifat rahasia		***teknologi informasi***

LAMPIRAN F : LAMPIRAN FORMULIR

Berikut ini adalah lampiran formulir yang dihasilkan dalam penelitian.

Formulir User Registration

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-01	NO. RILIS : NO. REVISI :
	FORMULIR USER REGISTRATION	TANGGAL TERBIT : HALAMAN :
FORMULIR		

UNTUK PEGAWAI

FORMULIR USER REGISTRATION
Nomor FM-01 - ... / ... / ...

Pemohon		
Nama	: bagus prasetyo	Tanda Tangan :
NIP	: 123452214551	
Jabatan	: Kepala Bagian Kepegawaian	
Unit Kerja	: Kepegawaian	
Email Aktif	: bagus@perbanas.ac.id	
Tanggal	: DDMMYYYY	
Buat Baru	: ☐ Ya ☐ Tidak	
Alasan Ganti	:	
		(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar F. 1 Formulir User Registration Untuk Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-01	NO. RILIS : NO. REVISI :
	FORMULIR USER REGISTRATION	TANGGAL TERBIT : HALAMAN :
FORMULIR		

UNTUK MAHASISWA

FORMULIR USER REGISTRATION
Nomor FM-01 - ... / ... / ...

Pemohon		
Nama	: adi hartanto	Tanda Tangan :
NRP	: 5212100027	
Angkatan	: 2012	
Fakultas	: Manajemen	
Jurusan	: Manajemen	
Email Aktif	: adi12@mhs.perbanas.ac.id	
Tanggal	: DDMMYYYY	
Buat Baru	: ☐ Ya ☐ Tidak	
Alasan Ganti	:	

(Lokasi), (Tanggal-Bulan-Tahun)
Staff TIK,

(Nama Lengkap Staff TIK)
NIP .....

Gambar F. 2 Formulir User Registration Untuk Mahasiswa

Formulir User De-registration

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-02	NO. RILIS : NO. REVISI :
	FORMULIR USER DE-REGISTRATION	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

UNTUK PEGAWAI

FORMULIR USER DE-REGISTRATION
Nomor FM-02 - ... / ... / ...

Pemohon		
Nama	: bagus prasetyo	Tanda Tangan :
NIP	: 123452214551	
Jabatan	: Kepala Bagian Kepegawaian	
Unit Kerja	: Kepegawaian	
Email Aktif	: bagus@perbanas.ac.id	
Tanggal non-aktif	:DDMMYYYY	
Alasan De-registrasi	:	
		(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar F. 3 Formulir User De-registration Untuk Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-02	NO. RILIS : NO. REVISI :
	FORMULIR USER DE-REGISTRATION	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

UNTUK MAHASISWA

FORMULIR USER DE-REGISTRATION
Nomor FM-02 - ... / ... / ...

Pemohon		
Nama	: adi hartanto	Tanda Tangan :
NRP	: 5212100027	
Angkatan	: 2012	
Fakultas	: Manajemen	
Jurusan	: Manajemen	
Email Aktif	: adi12@mhs.perbanas.ac.id	
Tanggal non-aktif	: DDMMYYYY	
Alasan De-registrasi	:	

(Lokasi), (Tanggal-Bulan-Tahun)
Staff TIK,

(Nama Lengkap Staff TIK)
NIP .....

Gambar F. 4 Formulir User De-registration Untuk Mahasiswa

Formulir Pendaftaran Akses Jaringan

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-03	NO. RILIS : NO. REVISI :
	FORMULIR PENDAFTARAN AKSES JARINGAN	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

UNTUK PEGAWAI

FORMULIR PENDAFTARAN AKSES JARINGAN
Nomor FM-03 - ... / ... / ...

Pemohon		
USER ID	: bagus@perbanas.ac.id	Tanda Tangan :
Nama	: bagus prasetyo	
NIP	: 123452214551	
Jabatan	: Kepala Bagian Kepegawaian	
Unit Kerja	: Kepegawaian	
Daftar Wifi (Diisi oleh staff)	:	
Daftar Layanan (Diisi oleh staff)	:	
Tanggal	: DDMMYYYY	

(Lokasi), (Tanggal-Bulan-Tahun)
Staff TIK,

(Nama Lengkap Staff TIK)
NIP .....

Gambar F. 5 Formulir Akses Jaringan Untuk Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-03	NO. RILIS : NO. REVISI :
	FORMULIR PENDAFTARAN AKSES JARINGAN	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

UNTUK MAHASISWA

FORMULIR PENDAFTARAN AKSES JARINGAN
Nomor FM-03 - ... / ... / ...

Pemohon		
USER ID	: adi12@mhs.perbanas.ac.id	Tanda Tangan :
Nama	: adi hartanto	
NRP	: 5212100027	
Angkatan	: 2012	
Fakultas	: Manajemen	
Jurusan	: Manajemen	
Daftar Wifi (Diisi oleh staff)	:	
Daftar Layanan (Diisi oleh staff)	:	
Tanggal	: DDMMYYYY	

(Lokasi), (Tanggal-Bulan-Tahun)
Staff TIK,

(Nama Lengkap Staff TIK)
NIP .....

Gambar F. 6 Formulir Akses Jaringan Untuk Mahasiswa

Formulir Perbaikan Sistem Informasi

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-04	NO. RILIS -
		NO. REVISI -
	FORMULIR PERBAIKAN SISTEM INFORMASI	TANGGAL TERBIT -
		HALAMAN -
	FORMULIR	

Laporan Perbaikan Sistem Informasi

Tanggal…. …. …. Bulan…. …. …. Tahun…. …. ….

Tanggal		Pukul	
Nama			
Unit Kerja			
Menu & Submenu yang diperbaiki			
Uraian Perbaikan			
REALISASI KERJA			
Analisis/Tinjuan (*disii oleh TIK*)			
Perbaikan (*disii oleh TIK*)			
Tanggal Mulai		Pukul	
Tanggal Selesai		Pukul	

Mengetahui,
Kepala Bagian TIK

(*Nama Lengkap Kepala Bagian TIK*)
NIP ……

(Lokasi), (Tanggal – Bulan – Tahun)
Pegawai Bagian TIK,

(*Nama Lengkap Pegawai Bagian TIK*)
NIP ……

Gambar F. 7 Formulir Perbaikan Sistem Informasi

Formulir Permintaan Pergantian Password

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-05	NO. RILIS :
		NO. REVISI :
	FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT :
		HALAMAN :
FORMULIR		

UNTUK PEGAWAI

FORMULIR PERMINTAAN PERGANTIAN PASSWORD
Nomor FM-05 - ... / ... / ...

Pemohon

Nama	: bagus prasetyo	Tanda Tangan :
NIP	: 123452214551	
Jabatan	: Kepala Bagian Kepegawaian	
Unit Kerja	: Kepegawaian	
Email Aktif	: bagus@perbanas.ac.id	
Tanggal	: DDMMYYYY	

Keterangan
(diisi dengan alasan permintaan pergantian password)

(Lokasi), (Tanggal-Bulan-Tahun)
Staff TIK,

(Nama Lengkap Staff TIK)
NIP .....

Gambar F. 8 Formulir Permintaan Pergantian Password Untuk Pegawai

	SEKOLAH TINGGI ILMU EKONOMI PERBANAS Bagian Teknologi Informasi dan Komunikasi (TIK)	
	FM-05	NO. RILIS : -
		NO. REVISI : -
	FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT :
		HALAMAN :
FORMULIR		

UNTUK MAHASISWA

FORMULIR PERMINTAAN PERGANTIAN PASSWORD
Nomor FM-05 - ... / ... / ...

Pemohon	
Nama :	Tanda Tangan :
NRP :	
Jurusan :	
Fakultas :	
Email Aktif :	
Tanggal :	
Keterangan (diisi dengan alasan permintaan pergantian password)	
	(Lokasi), (Tanggal-Bulan-Tahun) Staff TIK, (Nama Lengkap Staff TIK) NIP .....

Gambar F. 9 Formulir Permintaan Pergantian Password Untuk Mahasiswa

LAMPIRAN G : HASIL VERIFIKASI DAN VALIDASI SOP

Hasil Verifikasi SOP

Tabel dibawah ini berisikan penjelasan dari hasil verifikasi dokumen produk SOP Keamanan Aset Informasi Kendali Akses STIE Perbanas yang dilakukan dengan Kasie TIK STIE Perbanas. Verifikasi dokumen produk SOP dilakukan dengan teknik wawancara secara langsung.

Tanggal Wawancara : 14 Desember 2015
Nama Narasumber : Hariadi Yutanto, S.Kom, M.Kom
Peran Narasumber : Kasie TIK STIE Perbanas

Tabel G. 1 Verifikasi SOP

Pertanyaan	Jawaban
Menurut Bapak apakah kebijakan yang di rekomendasikan telah sesuai dengan kondisi pada STIE Perbanas? Atau adakah kebijakan yang kurang sesuai dan perlu diubah?	Karena secara spesifik belum ada kebijakan khusus mengenai Teknologi Informasi dan Komunikasi di STIE Perbanas ini, sehingga kebijakan yang direkomendasikan untuk dokumen SOP ini dapat diterima. Dan juga karena Bagian TIK juga sedang mengembangkan draft kebijakan untuk Blue Print TI, sehingga menurut saya beberapa kebijakan yang direkomendasikan ini dapat diterima dan diajukan untuk diimplementasikan.
Menurut Bapak apakah ada istilah yang kurang tepat yang digunakan dalam	Secara keseluruhan sudah tepat.

dokumen SOP ini?	
Apakah menurut Bapak ada aktivitas dalam SOP yang perlu diperbaiki atau ditambahkan?	Untuk beberapa aktivitas prosedur sudah benar namun pada prosedur permintaan pergantian password, mungkin bisa di spesifikan lagi karena untuk permintaan pergantian password mahasiswa dan dosen/pegawai alurnya berbeda. Beberapa dosen/pegawai apabila akan mengganti password dapat langsung meghubungi beberapa pegawai Bagian TIK melalui via telpon atau email dan lainnya.
Terakait dengan formulir dalam mendukung setiap prosedur yang dihasilkan apakah ada koreksi?	Untuk bagian formulir saya minta untuk diperbaiki bagian formulir User Registration, di dalam form nya ditambahkan saja ini permintaan hak akses baru atau sebelumnya sudah punya hak akses tapi ingin ganti. Kemudian ditambahkan lagi field alasan penggantian untuk nanti sebagai kolom user yang sudah punya hak akses tapi ingin mengganti.
	Setelah itu di bagian akses jaringan nanti ditambahkan saja kolom daftar hotspot/wifi dan daftar layanan, namun biarkan kolom itu nanti diisi oleh divisi kita supaya

	mengkelompokkannya mudah.
Terkait dengan instruksi kerja untuk pencegahan malware rekomendasi penggunaan *tools* nya apakah sudah sesuai?	Untuk *scanning* sebenarnya biasa dilakukan dengan *tools* Nicto. Namun rekomendasi ini bisa diterima.

Hasil Validasi Pengujian SOP

Berikut ini adalah lampiran yang berisi hasil skenario pengujian SOP beserta formulir-formulir yang diisi saat pengujian prosedur berlangsung.

1. Pengujian SOP Pendaftaran dan Penonaktifan Hak Akses

Tanggal Pengujian : 4 Januari 2016
Pelaksana :Yusuf Efendi, Pegawai Bagian TIK
Hariadi Yutanto, Administrator dan Kepala Bagian TIK
Bagus Prasojo, Mahasiswa STIE Perbanas

Hasil simulasi pengujian secara rinci akan dijelaskan dalam tabel berikut ini :

Tabel G. 2 Hasil Pengujian SOP Pendaftaran dan Penonaktifan Hak Akses

No.	Aktivitas	Keterangan
1.	Mengisi formulir pendaftaran/penghapusan hak akses	Bagus Prasojo pengisian formulir pendaftaran baru hak akses terlebih dahulu untuk diajukan ke bagian service desk
2.	Mengajukan permintaan ke Service Desk	Mahasiswa mengajukan formulir pendaftaran hak akses yang sudah diisi kepada bagian

No.	Aktivitas	Keterangan
		service desk
3.	Menyetujui, mencatat, dan meneruskan ke admin terkait	Yusuf effendi menerima permintaan pengajuan formulir pendaftaran hak akses, kemudian melakukan pencatatan dalam daftar permintaan hak akses setelah itu meneruskan permintaan tersebut kepada administrator
4.	Memverifikasi permintaan	Administrator melakukan pengecekan terhadap nama dan email pemohon sudah terdaftar di dalam system atau belum, dan memastikan belum memiliki hak akses
5.	Merekomendasikan persetujuan/penolakan permintaan	Administrator melakukan persetujuan terhadap permintaan yang diajukan oleh pemohon
6.	Persetujuan	Kepala bagian TIK melakukan persetujuan berdasarkan rekomendasi dari administrator
7.	Minta Admin mengalokasikan/menghapus hak akses	Admin mengalokasikan hak akses baru dengan memasukkan email pemohon
8.	Menyetujui/menghapus hak akses	Admin melakukan persetujuan pemberian

No.	Aktivitas	Keterangan
		hak akses kepada pemohon dan menyerahkan hak akses kepada yusuf effendi
9.	Mengkonfirmasikan status permintaan ke pemohon	Yusuf effendi melakukan panggilan kepada bagus untuk menyerahkan hak akses yang telah disetujui
10.	Menerima informasi status permintan	Bagus menerima hak akses terhadap fasilitas sistem informasi yang ada di STIE Perbanas

2. Pengujian SOP Pendaftaran Akses Jaringan

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Yusuf Efendi, Pegawai Bagian TIK
Hariadi Yutanto, Administrator dan Kepala Bagian TIK
Bagus Prasojo, Mahasiswa STIE Perbanas

Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 3 Pengujian SOP Pendaftaran Akses Jaringan

No.	Aktivitas	Keterangan
1.	Mendapatkan permintaan akses ke layanan jaringan dan formulir berupa e-mail dari Intranet Perbanas	Bagus mengakses menggunakan salah satu wifi di STIE Perbanas namun gagal dan muncul pemberitahuan untuk meminta izin akses wifi
2.	Mengisi formulir	Bagus meminta dan melakukan pengisian

No.	Aktivitas	Keterangan
		formulir akses jaringan kepada yusuf effendi
3.	Mencatat data pengisi formulir	Service desk melakukan pencatatan data pemohon dan kemudian meneruskan formulir tersebut kepada admin
4.	Menerima formulir	Admin menerima formulir dari service desk kemudian melakukan pencatatan layanan dan wifi mana saja yang bisa diakses oleh pemohon
5.	Meminta persetujuan	Admin mengajukan persetujuan kepada Kepala TIK
6.	Persetujuan	Kepala TIK melakukan persetujuan terhadap permintaan yang diajukan oleh admin
7.	Admin memberikan akses jaringan yang diminta per formulir permintaan	Admin memberikan formulir persetujuan kepada bagian service desk
8.	Mengembalikan permintaan	Yusuf effendi melakukan pencatatan formulir persetujuan kemudian menyerahkan daftar layanan dan wifi yang bisa diakses oleh pemohon
9.	Menerima kembali permintaan yang diajukan	Bagus menerima akses jaringan sistem informasi yang ada di STIE Perbanas

3. Pengujian SOP Manajemen Password

Tanggal Pengujian : 4 Januari 2016
Pelaksana : Yusuf Effendi, Pegawai Bagian TIK, Bagus Prasojo, Mahasiswa STIE Perbanas

Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel G. 4 Hasil pengujian SOP Manajemen Password

No	Aktivitas	Keterangan
Proses Pengelolaan Password		
1	Mempersiapkan prosedur perubahan *password* lama dan melakukan *setup* pada seluruh sistem.	Proses persiapan termasuk *coding* penambagan fitur pada sistem informasi kepegawaian uji coba (bajool.perbanas.ac.id) telah dilakukan
2	Menyediakan *password default* sementara yang telah sesuai dengan standar *strong password* untuk masing masing pengguna sistem	Password default untuk pegawai telah disiapkan, namun hanya sebatas untuk pegawai bagian TIK sebagai uji coba
3	Mensosialisasikan penambahan fitur baru kepada seluruh civitas akademika melalui website resmi	Tidak dilakukan, karena prosedur yang dilakukan hanya sebatas uji coba
4	Mengirimkan *email* yang berisikan *password default* sementara untuk seluruh pengguna sistem dan informasi mengenai ketentuan penggunaan kualitas standard *strong password*	Email pegawai didapatkan dari database pegawai dan email pemberitahuan pergantian fitur dalam sistem informasi berhasil dikirimkan, namun sebatas hanya

No	Aktivitas	Keterangan
		pada salah satu pegawai TIK
5	Salah satu pegawai Bagian TIK lain sebagai pengguna sistem informasi kepegawaian mencoba melakukan *log in*.	Pegawai bagain TIK lain berhasil mengakses email dan melakukan log in pada sistem kepegawaian uji coba
6	Sistem menampilkan notifikasi untuk meminta civitas akademika melakukan pergantian *password default* dengan *password* baru yang sesuai dengan ketentuan kualitas standard *strong password*	Sistem berhasil menapilkan permintaan pergantian password
7	Mengelola data penggunaan password lama dan memastikan tidak ada penggunaan kembali *password default*	Tidak dilakukan
Proses Permintaan Pergantian Password		
1	Pengguna sistem melakukan permintaan pergantian *password (*dalam simulasi ini pengguna adalah pegawai bagian TIK*)*	Bagus Prasojo salah satu mahasiswa STIE Perbanas datang ke bagian TIK dengan membawa surat persetujuan permintaan pergantian password
2	Mahasiswa selanjutnya mengisi formulir permintaan pergantian password dengan menyertakan alasan permintaan pergantian *password*	Mahasiswa mengisi formulir permintaan pergantian password
3	Pegawai Bagian TIK melakukan validasi pada	Pegawai Bagian TIK melakukan validasi

No	Aktivitas	Keterangan
	formulir permintaan pergantian password	formulir permintaan pergantian password
4	Pegawai Bagian TIK kemudian mengirimkan *email* yang berisikan *link* untuk menginputkan *password* baru kepada pengguna sistem yang melakukan permintaan pergantian *password*	Pegawai Bagian TIK kemudian mengirimkan email untuk mahasiswa berdasarkan kolom email yang ada pada formulir
5	Pengguna Sistem kemudian mengakses *link* dan menginputkan *password* baru	Berhasil dilakukan oleh mahasiswa
6	Sistem selanjutnya melakukan verifikasi dan validasi inputan *password* baru	Sistem berhasil memverifikas password baru dan password ter-*record* dalam database mahasiswa

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang dibuat adalah jawaban dari perumusan masalah yang telah didefinisikan sebelumnya dan berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan yang didapat dari tahap analisis hingga perancangan dan validasi dokumen produk adalah :

1. **Analisis risiko keamanan aset informasi terkait kendali akses STIE Perbanas Surabaya berdasarkan tahap penilaian risiko pada kerangka kerja ISO/IEC:27002:2013**

   Analisis risiko dilakukan dengan menggunakan metode FMEA dan menganalisis ancaman serta kerentanan dari aset informasi yaitu Sumber daya Manusia, Data, dan Software. Berdasarkan hasil analisis penilaian risiko, dapat diketahui bahwa STIE Perbanas Surabaya memiliki beberapa kemungkinan risiko yang tinggi yang dapat timbul terkait keamanan aset informasi kendali akses, risiko tersebut muncul dikarenakan oleh berbagai penyebab seperti serangan *hacker,* dan *human error.* Sehingga dari hasil penelitian, risiko yang memiliki prioritas paling tinggi adalah sebagai berikut :

   1. Sharing password antara mahasiswa/i
   2. Username dan password diketahui oleh pengguna lain
   3. Terdapat hacker yang memanipulasi data
   4. Terdapat hacker yang mencuri data
   5. Kesalahan dalam pemberian hak akses

2. **Hasil Pembuatan *Standard Operating Procedure* (SOP) Keamanan Aset Informasi Berdasasarkan Kendali Akses Dengan Menggunakan ISO/IEC:27002:2013 Pada Studi Kasus STIE Perbanas Surabaya**
   Berdasarkan hasil analisis risiko dan rekomendasi mitigasi risiko, didapatkan usulan pembuatan 3 kebijakan dan 3 prosedur yaitu 1) Kebijakan Kendali Akses 2) Kebijakan Tanggung Jawab Pengguna Teknologi Informasi 3) Kebijakan Secure Log-on 4) SOP Pendaftaran dan Penonaktifan Hak Akses 5) SOP Pendaftaran Akses Jaringan 6) SOP Manajemen Password.

   Selain 3 kebijakan dan 3 prosedur tersebut, dihasilkan juga beberapa instrument pendukung dokumen SOP berupa formulir untuk melengkapi dokumen SOP tersebut. Formulir yang dihasilkan antara lain 1) Formulir User Registration 2) Formulir User De-registration 3) Formulir Pendaftaran Akses Jaringan 4) Formulir Perbaikan Sistem Informasi dan 5) Formulir Permintaan Pergantian Password. Keseluruhan isi dokumen SOP dibukukan secara terpisah dari buku tugas akhir ini dan menjadi sebuah dokumen produk berjudul **Standard Operating Procedure (SOP) Kendali Akses STIE Perbanas.**

3. **Hasil Verifikasi dan Validasi Dokumen SOP Kendali Akses Pada Studi Kasus STIE Perbanas Surabaya**
   Pada proses verifikasi dokumen SOP yang dilakukan terdapat beberapa perubahan dari dokumen awal yang sudah dibuat, perubahan tersebut terletak pada **Formulir User Registration**, perubahan tersebut berupa penambahan *field* (buat baru, dan alasan ganti), dan juga **Formulir Pendaftaran Akses Jaringan**, perubahan tersebut berupa penambahan *field* (daftar wifi, dan daftar layanan). Sedangkan pada proses validasi hanya dilakukan pada prosedur saja, diantaranya ada **SOP Pendaftaran dan Penonaktifan Hak Akses, SOP Pendaftaran Akses**

Jaringan, dan SOP Manajemen Password. Beberapa SOP tersebut diberlakukan batasan dalam melakukan validasi dikarenakan pertimbangan efisiensi waktu dan juga keterbatasan sumber daya. Hasil dari validasi tersebut semua scenario tersebut dilaksanakan dengan baik.

7.2 Saran

Saran yang dapat peneliti sampaikan terkait dengan pengerjaan tugas akhir ini meliputi dua hal, yaitu saran untuk pihak manajemen STIE Perbanas dan saran untuk penelitian selanjutnya.

Saran yang dapat diberikan untuk pihak manajemen STIE Perbanas adalah :

1. Penulis menyarankan agar pihak STIE Perbanas melakukan rencana penerapan dan melakukan sosialisasi pada seluruh pihak yang terkait pada seluruh pelaksanaan SOP yang telah dibuat
2. Usulan formulir yang telah dibuat dapat diimplementasikan dengan baik untuk mengelola aset-aset sistem informasi sehingga aset-aset bisa terkelola secara terstruktur dan terdokumentasi dengan baik
3. Penerapan kebijakan dapat diimplementasikan kepada seluruh civitas akademika yang ada di STIE Perbanas. Langkah yang sebaiknya diambil selanjutnya adalah mengambil kebijakan yang tepat dengan kondisi yang ada saat ini di STIE Perbanas agar bisa diimplementasikan dengan tepat guna.

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah :

1. Penelitian ini sebatas pembuatan dokumen SOP hingga proses pengujian tanpa memantau pengimplementasian SOP tersebu dan pengaruhnya bagi proses bisnis organisasi. Untuk penelitian selanjutnya, dapat dilakukan pengujian dan evaluasi keefektifan dokumen SOP ini terhadap peningkatan

keamanan aset informasi terkait kendali akses pada STIE Perbanas Surabaya.

2. Penelitian ini hanya mengacu pada kontrol kerangka kerja ISO/IEC:27002:2013 dan tidak secara keseluruhan memenuhi salah satu domain atau klausul pada kerangka kerja tersebut, karena pada dasarnya penelitian ini didasarkan pada hasil penilaian risiko untuk melakukan mitigasi pada risiko dengan tingkat prioritas tertinggi. Sehingga dalam penelitian selanjutnya dianjurkan untuk melengkapi objektif pada salah satu domain atau klausul pada kerangka kerja sehingga kontrol dalam penyusunan SOP lebih menyeluruh dan patuh.

DAFTAR PUSTAKA

[1] ISO/IEC27001. (2013). *Information Technology – Security Techniques – Information Security Management System Requirements.* Switzerland: ISO/IEC 2013.

[2] Sarno, R. & Iffano, I. *Sistem Manajemen Keamanan Informasi*. Surabaya, Indonesia: ITS Press.

[3] DataLossDB. (2011). *DataLossStatistics.* Retrieved October 27, 2012, from Data Loss Database: http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year

[4] R Stup. (2002). Standard Operating Procedures: Managing The Human Variables. *National Mastitis Council Regional Meeting Proceedings.*

[5] Utomo, M., Noor Ali, A.H., & Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS Vol. 1 No 1*, A288 – A293.

[6] Pandu Gilas Anarkhi, Noor Ali, A.H., & Kurnia, Indah. (2013). Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC 27001 Klausul Kendali Akses. *Jurnal Teknik Pomits Vol. 1, No. 1,* (2013) 1-5.

[7] Nur Fatimah, Aulia. (2015). Pembuatan Dokumen SOP (Standard Operating Procedure) Keamanan Data Yang Mengacu Pada Kontrol Kerangka Kerja Cobit 5 Dan ISO 27002:2013 (Studi Kasus : STIE Perbanas). *Jur. Sist. Inf. ITS,* Vol. 1, 2015.

[8] " Definisi Aset dan Liabilities | Liza Muzayana – Academia.edu " [Online] Available:

http://www.academia.edu/5442275/Definisi_Aset_dan_Liabilities

[9] Rohmani, Asih. (2014). "Proteksi Aset Informasi". Semarang, Indonesia : Udinus Repository.

[10] " ISO 17799: Standar Sistem Manajemen Keamanan Informasi | Melwin Syafrizal – Academia.edu " [Online] Available: http://www.academia.edu/5082000/ISO_17799_Standar_Sistem_Manajemen_Keamanan_Informasi

[11] Anderson, Ross J., (2008). " Security Engineering : A Guide to Building Dependable Distributed Systems ". England. Wiley.

[12] Saltzer, Jerome H., & Schroeder Michael D., (1975). *The Protection of Information in Computer Systems*. United States of America. University of Virginia, Departmen of Computer Science.

[13] Vaughan, Emmet J., & Elliot, Curtis M., (1978). *Fundamental of Risk and Insurance.* New York. John Willey & Sons Inc.

[14] Westerman, George & Hunter, Richard. (2007). *IT Risk: Turning Business Threats into Competitive Advantage.* United States of America. Harvard Business School Press.

[15] Djohanputro, B. (2008). Manajemen Risiko Korporat. *Pendidikan dan Pembinaan Manajemen.*

[16] Rama, Dasaratha V., & Jones, Frederick L. (2008). *Sistem Informasi Akuntansi*. Indonesia. Salemba Empat.

[17] Blokdijk, Gerrard. (2008). *IT Risk Management Guide.* Australia. Emereo Publishing

[18] Panda, P. (2005). The OCTAVE Approach to Information Security Risk Assessment. *ISACA Journal Vol. 4.*

[19] Christoper J. Alberts, S. B. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework.* Canada: Software Engineering Institure.

[20] Akyar, I. (2012). *Standard Operating Procedures (What Are They Good For).* Turkey

[21] KPRS. (2013). *Pedoman Pembuatan Standard Operating Procedures (SOP).* Jakarta: Pusat da Informasi

[22] USEP. (2007). *Guidence for Preparing Standard Operating Procedures (SOP).* Washington: Office of Environmental Information.

(halaman ini sengaja dikosongkan)

BIODATA PENULIS

Penulis bernama lengkap Ardhana Yudi Saputra, biasa dipanggil Ardhana. Penulis dilahirkan di Madiun pada hari Rabu Tanggal 29 Desember 1993 dan merupakan anak pertama dari dua bersaudara. Penulis telah menempuh pendidikan formal di MIN Takeran, tamat SMP di SMPN 1 Madiun, tamat SMA di SMAN 3 Madiun, dan kemudian masuk perguruan tinggi negeri ITS Surabaya pada jurusan Sistem Informasi (SI), Fakultas Teknologi Informasi pada tahun 2012. Adapun pengalaman yang didapatkan penulis selama di ITS, yakni berkecimpung di organisasi kemahasiswaan di jurusan SI selama satu tahun kepengurusan dan juga di lingkup UKM selama 2 tahun kepengurusan. Penulis pernah menjalani kerja praktik di Industri Kereta Api Indonesia (INKA) pada divisi IT selama kurang lebih 1,5 bulan pada tahun 2015. Pengalaman yang didapatkan penulis selama bekerja praktik yaitu membangun sebuah analisis desain perangkat lunak beserta pembuatan perangkat lunak untuk sistem barcoding pada proses pengerjaan material yang ada di INKA Madiun.

Pada pengerjaan Tugas Akhir di Jurusan Sistem Informasi ITS, penulis mengambil bidang minat Manajemen Sistem Informasi dengan topik Manajemen Risiko TI, Tata Kelola TI dan Keamanan Aset Informasi, yakni pembuatan Standar Operating Procedure Keamanan Aset Informasi Berdasarkan Kendali Akses Dengan Menggunakan ISO/IEC:27002:2013 Pada Studi Kasus STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas Surabaya. Untuk menghubungi penulis, dapat melalui email di ardhana29@gmail.com